OVERVIEW OF VIRTUAL SECURITY HOME LAB

This home lab is created for homelab security undersanding how network level is used. This home lab can be created in vm ware or virtual box. In this lab setup is done for pfsense, kali, active directory,metasploit,ubantu splunk,malware analysis,threat detection.

System Requirements

16GB RAM

256GB storage or maximum

64-bit multi-threaded CPU (minimum 4 cores)

***First we have to install Virtual Box in Our System ***

***Then set up proper extension for virtualbox ***

Pfsense installation steps

First you have to install PFSENSE iso file. you can refer this link given in down :

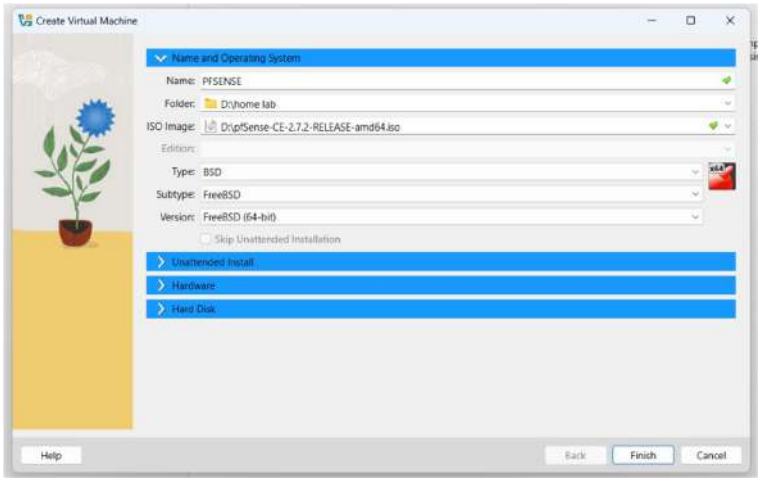
https://atxfiles.netgate.com/mirror/downloads/pfSense-CE-2.7.2-RELEASE-amd64.iso.gz

The downloaded file will have the extension **.iso.gz**. Use a decompression software like **Zipextractor** to extract the image.

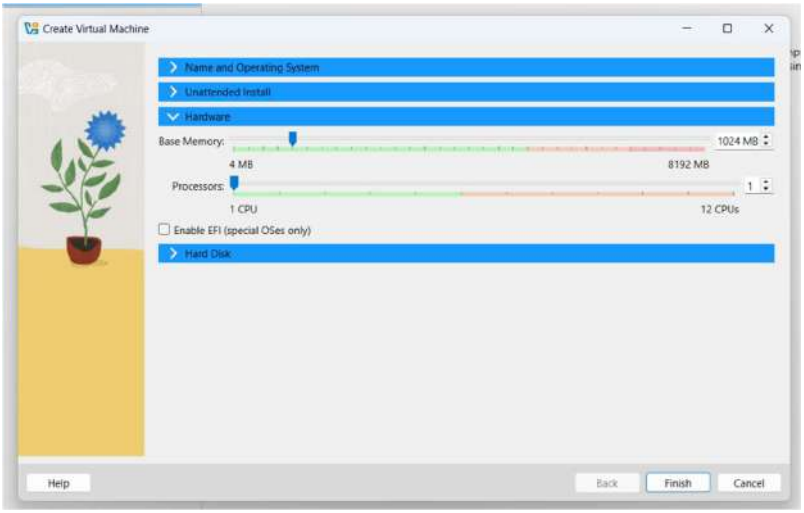
After extracting, you'll get a **.iso** file.

Open VirtualBox → Click **Tools** → Click **New**.

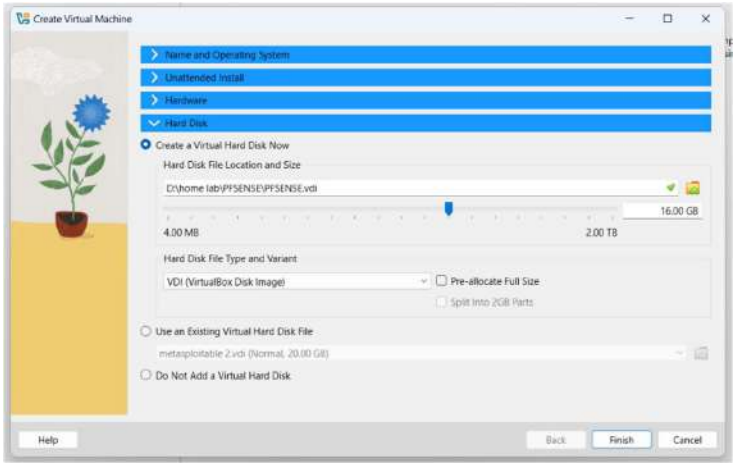
Enter a **name**, choose a **folder**, select **ISO Image → Others → your .iso file**, set **Type: BSD**, **Version: FreeBSD (64-bit)**, then click **Next**. ✅



Click next

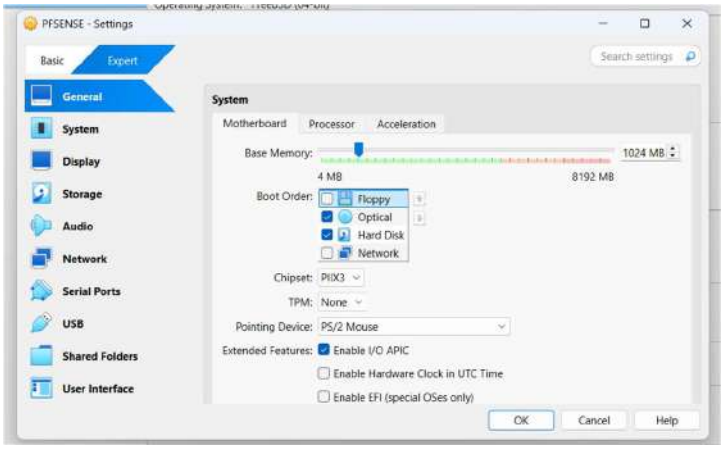


Click finish

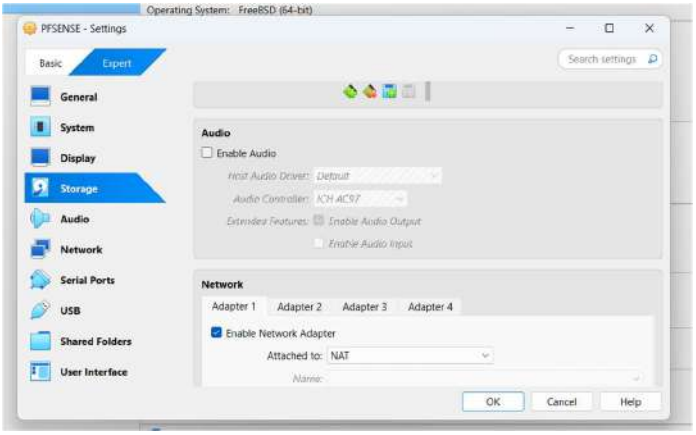


Click on settings after virtual machine added

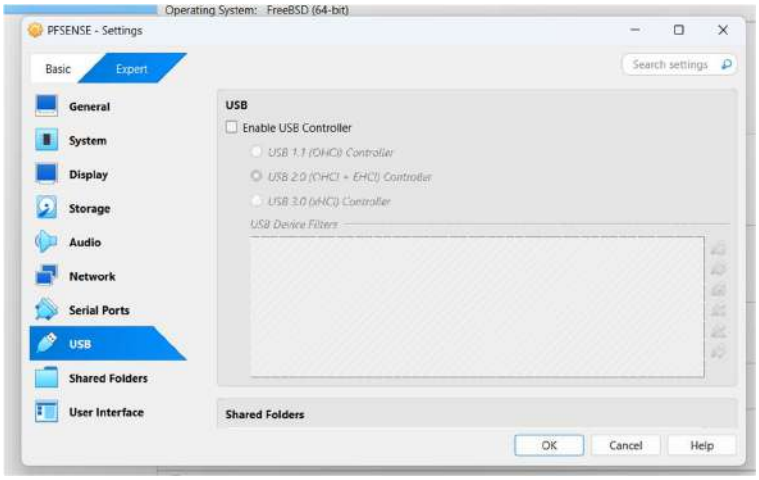
Then click system option after clicking system option then untick floppy disk



Then click Audio and untick it

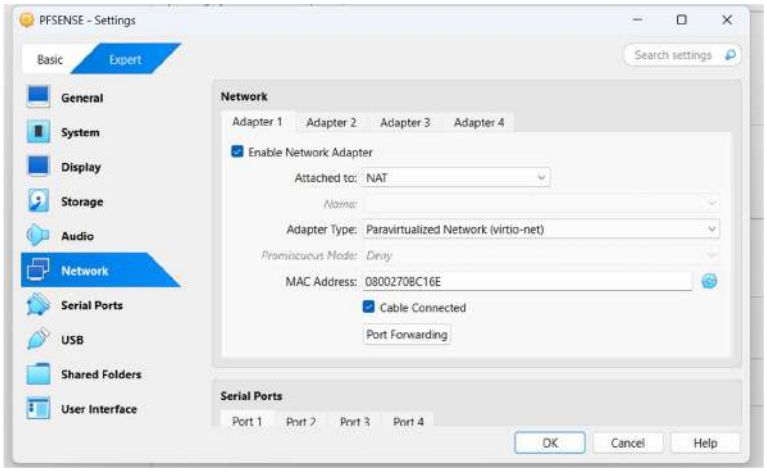


After we have to untick USB also

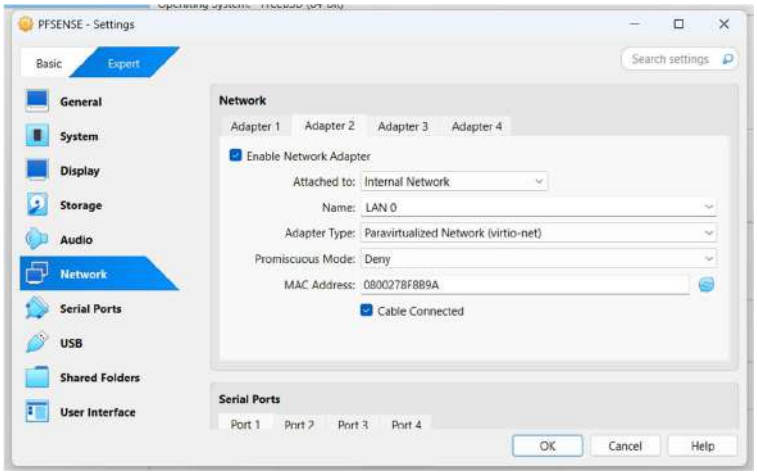


In last we are adding networks

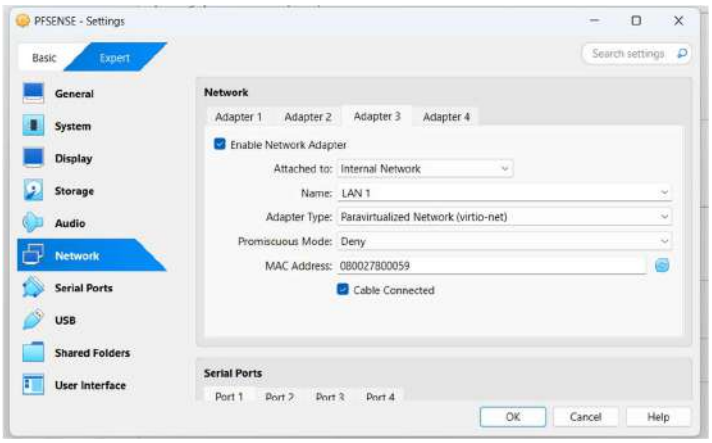
Network → Adapter 1 → Set **Attached to: NAT →** Expand **Advanced →** Set **Adapter Type: Paravirtualized Network (virtio-net)**.



Adapter 2 → Enable **Network Adapter →** Set **Attached to: Internal Network →** Name: **LAN 0 →** Expand **Advanced →** Set **Adapter Type: Paravirtualized Network (virtio-net)**.

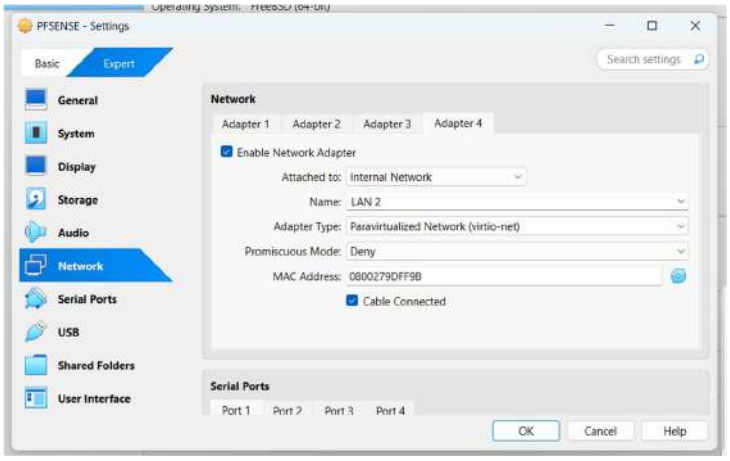


Adapter 3 → Enable **Network Adapter** → Set **Attached to: Internal Network** → Name: **LAN 1** → Expand **Advanced** → Set **Adapter Type: Paravirtualized Network (virtio-net)**.



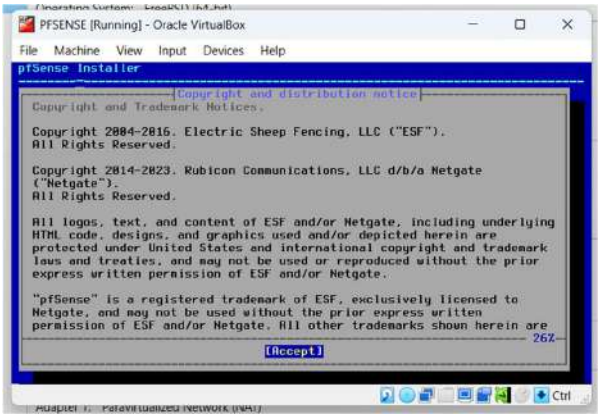
Adapter 4 → Enable **Network Adapter** → Set **Attached to: Internal Network** → Name: **LAN 2** → Expand **Advanced** → Set **Adapter Type: Paravirtualized Network (virtio-net)**.

Click **OK** to save and exit.

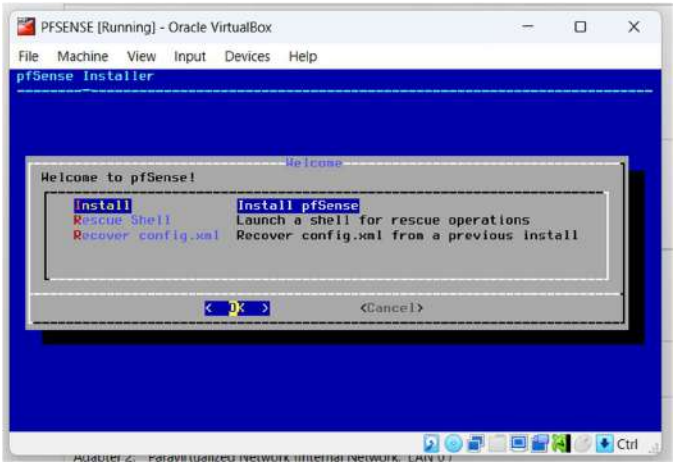


Select the pfSense VM from the sidebar and click on **Start** from the toolbar.

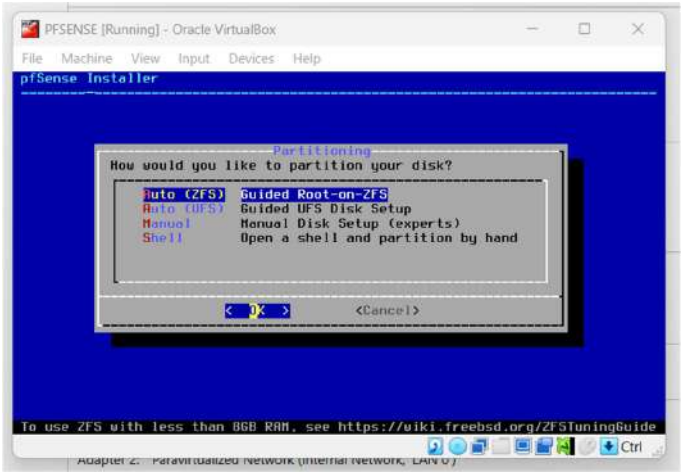
Wait for the text to finish loading, then press **Enter** to accept the agreement.



Press **Enter** to start the Installation.

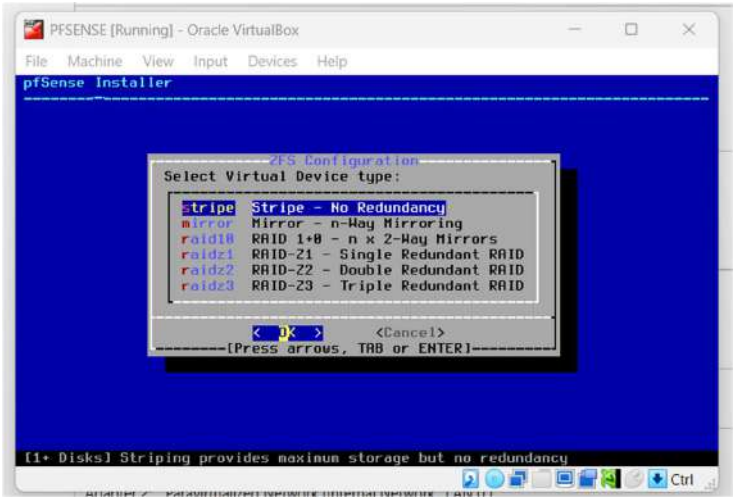


Press **Enter** to select the Auto (ZFS) partition option.

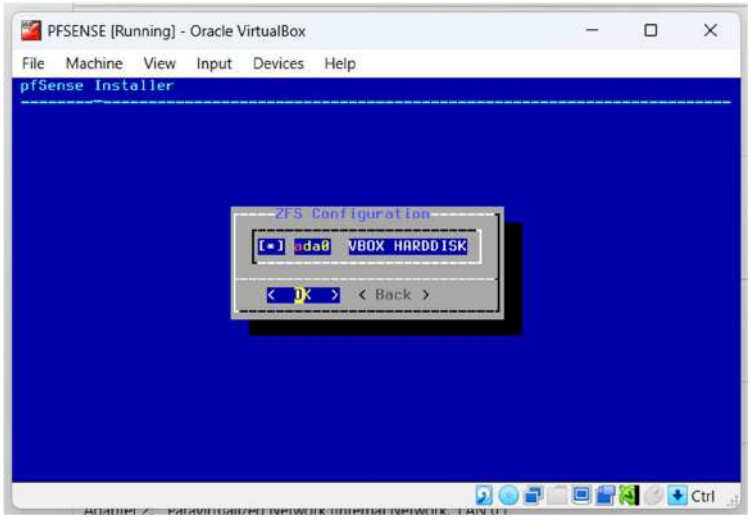


Press **Enter** to select Proceed with Installation.

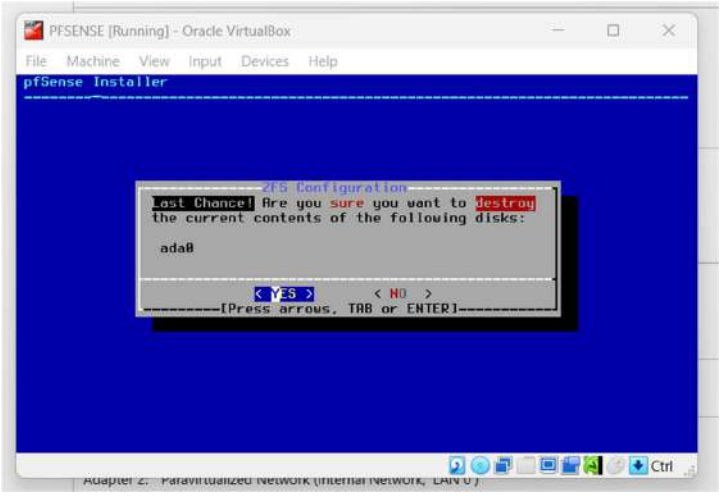
Press **Enter** to select Stripe - No Redundancy.



Use the **Spacebar** key to select the Hard Drive (**ada0**) then press **Enter** to continue.

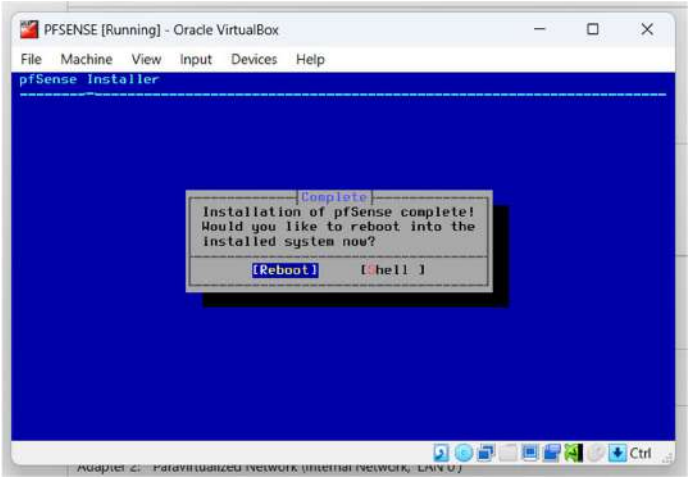


Use the Left Arrow to select **YES** and then press **Enter** to continue.



Wait for the installation to complete.

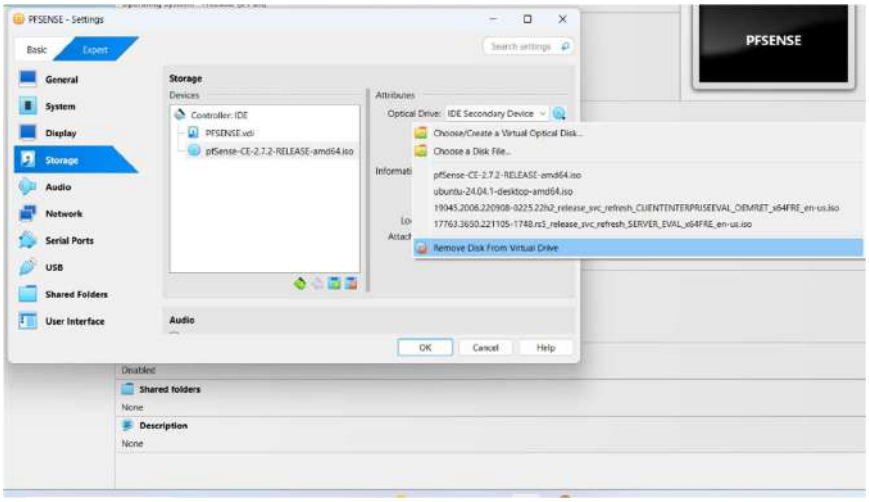
Press **Enter** to Reboot the VM.



After the VM is shut down. Click on **Settings** from the toolbar.

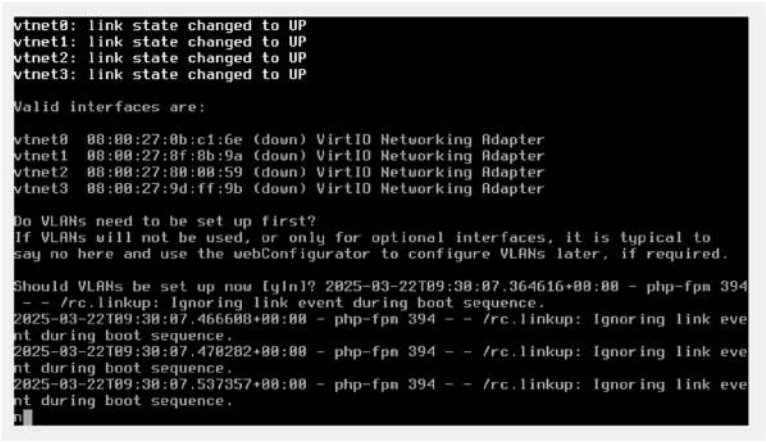
Go to the **Storage** tab. In the Storage Devices section click on the pfSense **.iso** image then click on the small disk image on the right side of the Optical Drive option.

From the dropdown select **Remove Disk from Virtual Drive**. Click on **OK** to save the changes and close the configuration menu.



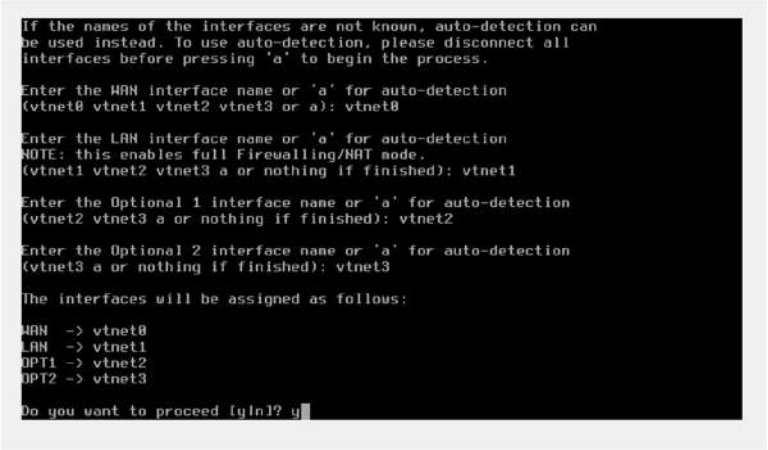
Then start vm . After starting vm then

Should VLANs be set up now? **n**
In the next step, we will configure the interfaces manually.



Enter the WAN interface name: **vtnet0**
Enter the LAN interface name: **vtnet1**
Enter the Optional 1 interface name: **vtnet2**
Enter the Optional 2 interface name: **vtnet3**

Do you want to proceed?: **y**

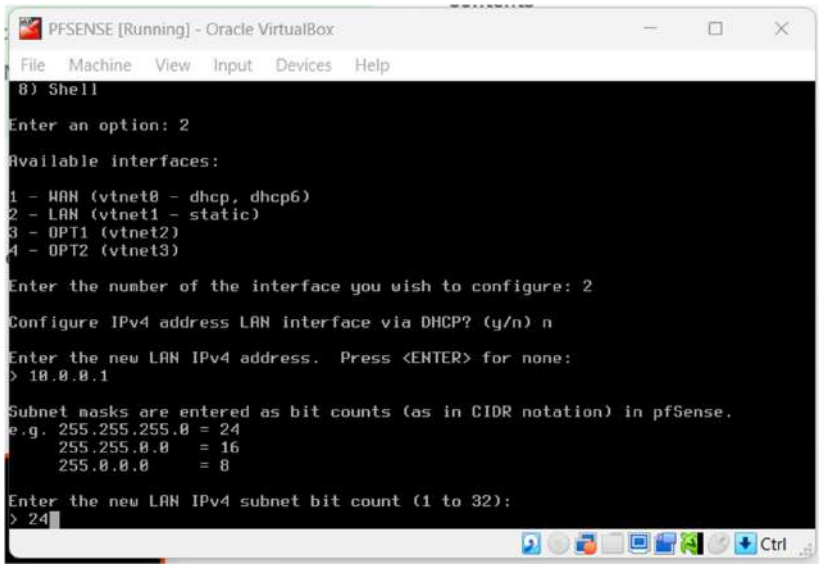


Set **static IPv4 addresses** for **LAN, OPT1, and OPT2** to prevent changes on reboot.

Configuring LAN (vtnet1)

Enter **2** to select "Set interface(s) IP address". Enter **2** to select the **LAN** interface.

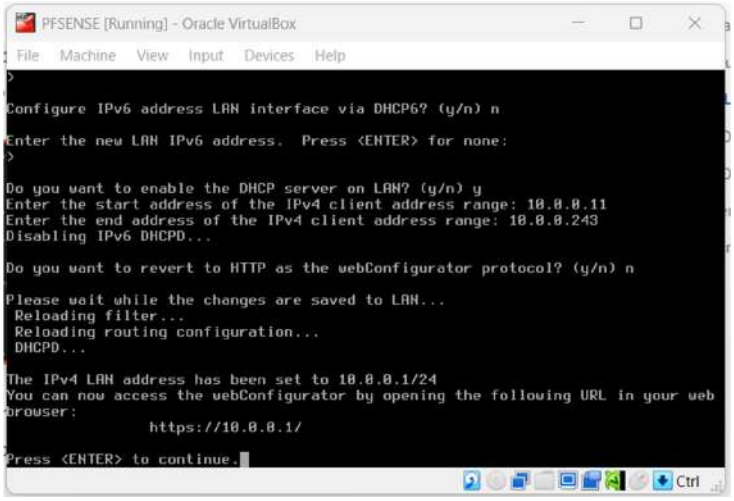
Configure IPv4 address LAN interface via DHCP?: **n**
Enter the new LAN IPv4 address: **10.0.0.1**
Enter the new LAN IPv4 subnet bit count: **24**



For the next question directly press **Enter**. Since this is a **LAN** interface we do not have to worry about configuring the upstream gateway.

Configure IPv6 address LAN interface via DHCP6: **n**
For the new LAN IPv6 address question press **Enter**
Do you want to enable the DHCP server on LAN?: **y**
Enter the start address of the IPv4 client address range: **10.0.0.11**
Enter the end address of the IPv4 client address range: **10.0.0.243**
Do you want to revert to HTTP as the webConfigurator protocol?: **n**

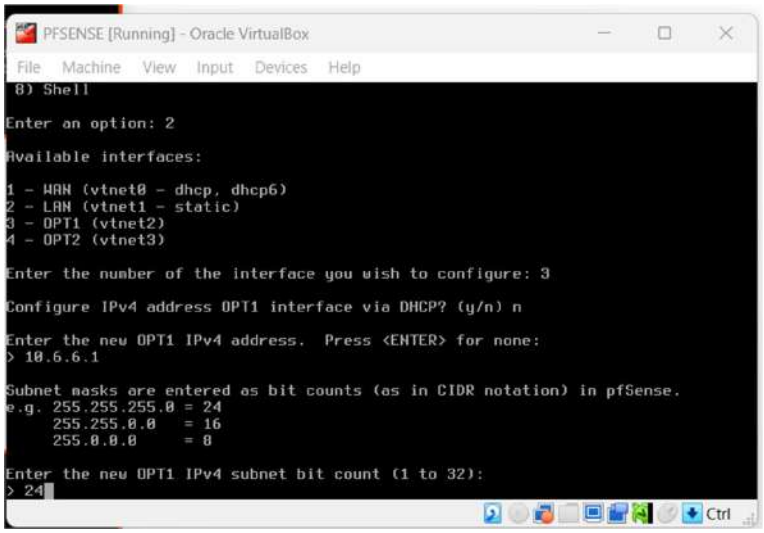
Press **Enter** to complete the **LAN** interface configuration.



Configuring OPT1 (vtnet2)

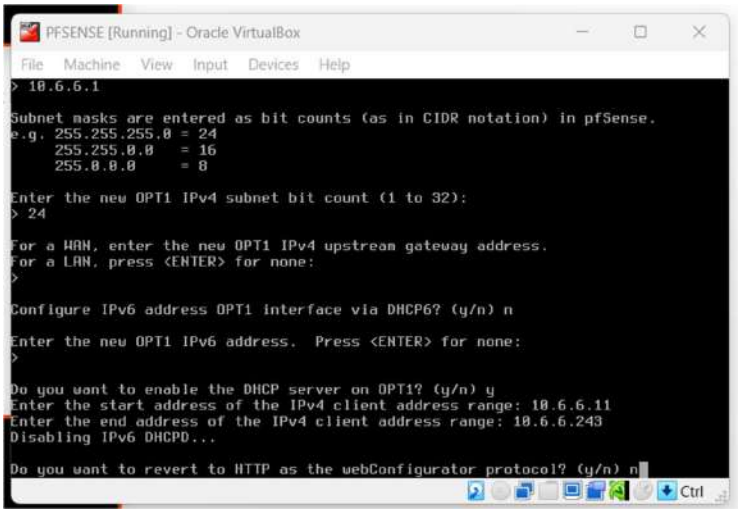
Enter **2** to select "Set interface(s) IP address". Enter **3** to select the **OPT1** interface.

Configure IPv4 address OPT1 interface via DHCP?: **n**
Enter the new OPT1 IPv4 address: **10.6.6.1**
Enter the new OPT1 IPv4 subnet bit count: **24**



For the next question directly press **Enter**. Since **OPT1** is a **LAN** interface we do not have to worry about configuring the upstream gateway.

Configure IPv6 address OPT1 interface via DHCP6: **n**
For the new OPT1 IPv6 address question press **Enter**
Do you want to enable the DHCP server on OPT1?: **y**
Enter the start address of the IPv4 client address range: **10.6.6.11**
Enter the end address of the IPv4 client address range: **10.6.6.243**
Do you want to revert to HTTP as the webConfigurator protocol?: **n**

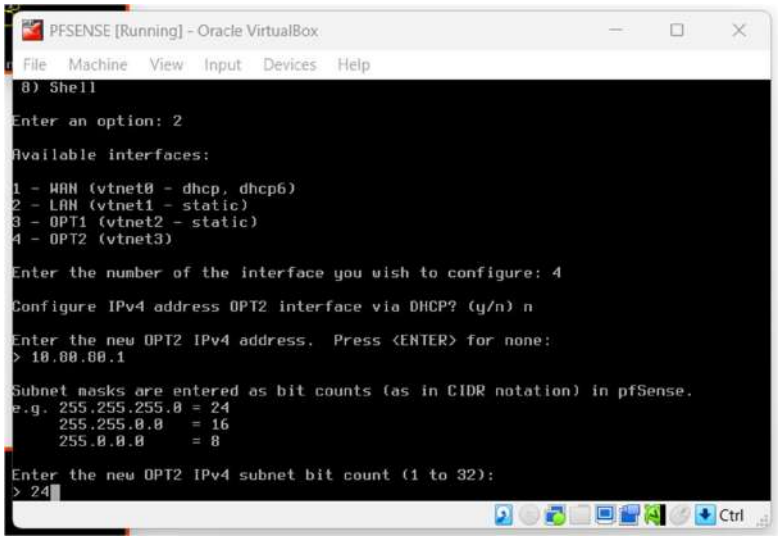


Press **Enter** to save the changes and return to the main menu.

Configuring OPT2 (vtnet3)

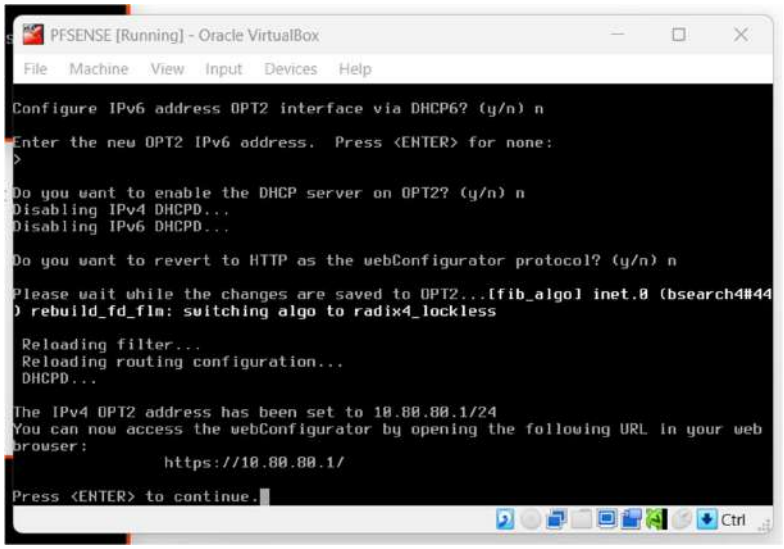
Enter **2** to select "Set interface(s) IP address". Enter **4** to select the **OPT2** interface.

Configure IPv4 address OPT2 interface via DHCP?: **n**
Enter the new OPT2 IPv4 address: **10.80.80.1**
Enter the new OPT2 IPv4 subnet bit count: **24**



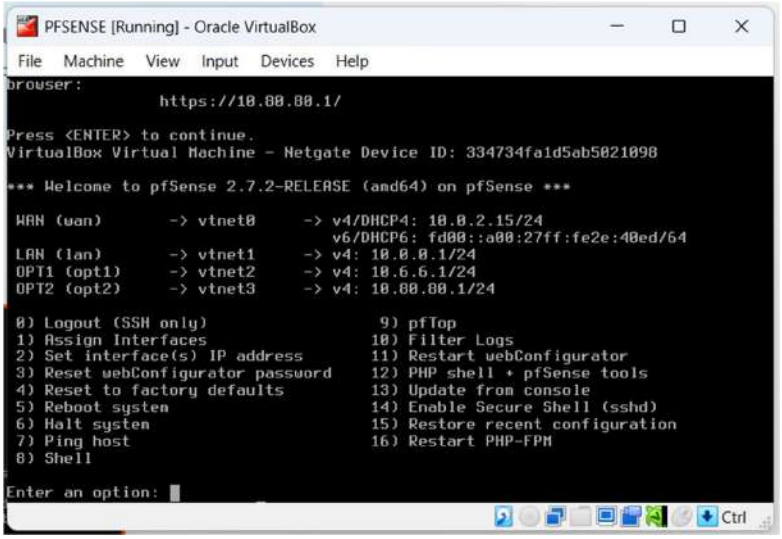
For the next question directly press **Enter**. Since **OPT2** is a **LAN** interface we do not have to worry about configuring the upstream gateway.

Configure IPv6 address OPT2 interface via DHCP6: **n**
For the new OPT2 IPv6 address question press **Enter**
Do you want to enable the DHCP server on OPT2?: **n**
Do you want to revert to HTTP as the webConfigurator protocol?: **n**



Press **Enter** to save the changes and return to the main menu.

The IP addresses for the **LAN**, **OPT1** and **OPT2** interfaces should be as follows:



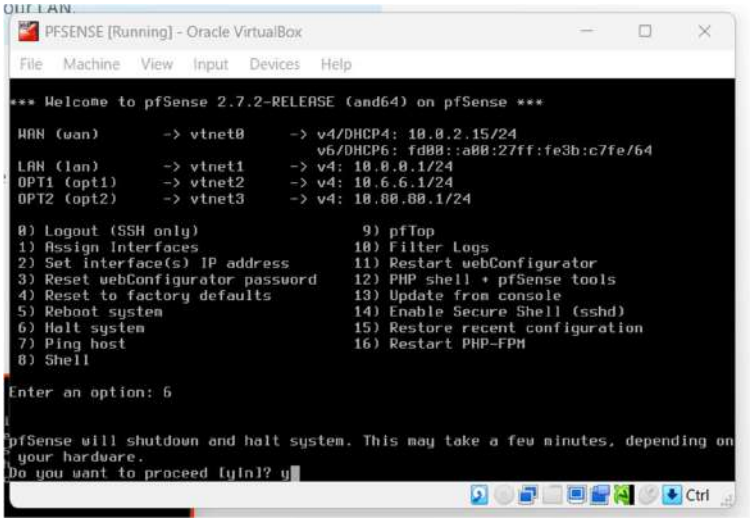
Interface setup in **pfSense** is complete.

Next, we'll set up **Kali Linux** and use it to access the **pfSense Web Interface** for further configuration.

Shut down pfsense

Enter a option: **6** (Halt system) Do you want to process?: **y**

This will initiate the shutdown sequence.


PFSENSE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> vtnet0 -> v4/DHCP4: 10.0.2.15/24
v6/DHCP6: fd00::a00:27ff:fe3b:c7fe/64
LAN (lan) -> vtnet1 -> v4: 10.0.0.1/24
OPT1 (opt1) -> vtnet2 -> v4: 10.6.6.1/24
OPT2 (opt2) -> vtnet3 -> v4: 10.80.80.1/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option: 6
pfSense will shutdown and halt system. This may take a few minutes, depending on your hardware.
Do you want to proceed [yln]? y
Ctrl

KALI INSTALLATION

FOR kali installation we directly use prebuilt virtual box machine

We can download from - https://www.kali.org/get-kali/#kali-virtual-machines this site

We are downloading virtual box machine

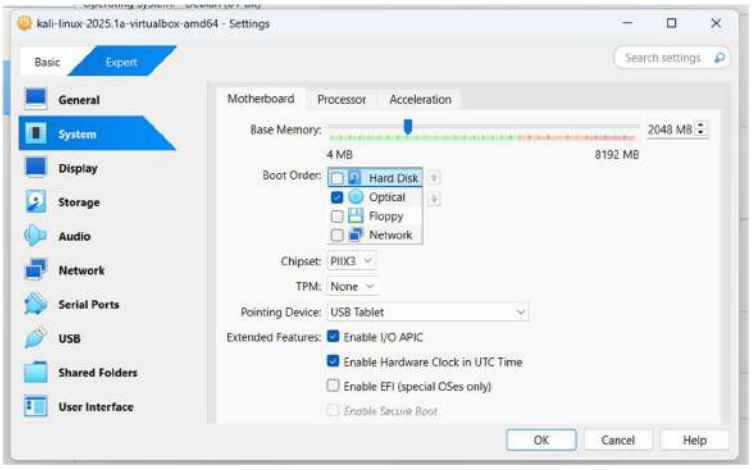
After installation unzip kali virtual box machine

Then open virtual box and select add option from tools

Then select downloaded kali virtual machine file

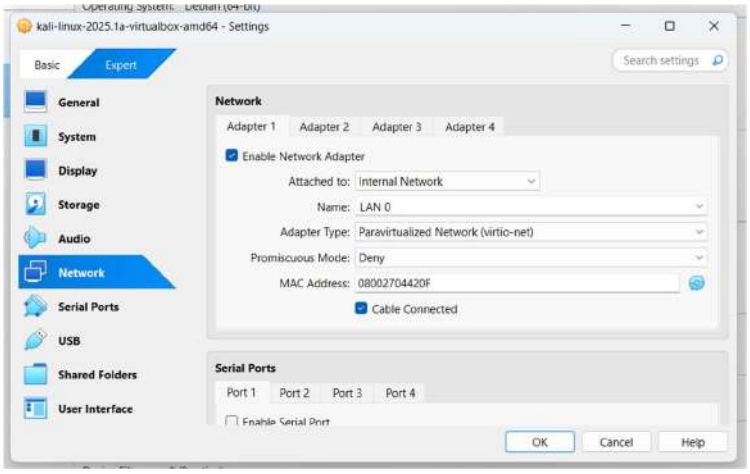
After that it get installed without extra step

Go to **System -> Motherboard**. For the Boot Order option ensure that the **Hard Disk** is on the top followed by **Optical**. Uncheck **Floppy**.



Network Configuration

Go to **Network -> Adapter 1**. For the Attached to field select **Internal Network**.
For Name select **LAN 0**. Expand the Advanced section. For Adapter Type select **Paravirtualized Network (virtio-net)**.

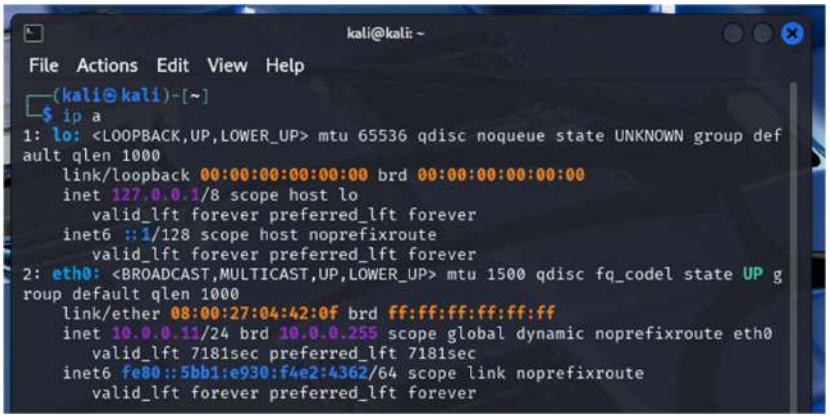


Then start kali machine

Login by using default username and password : kali {default}

Then open terminal and check ip address

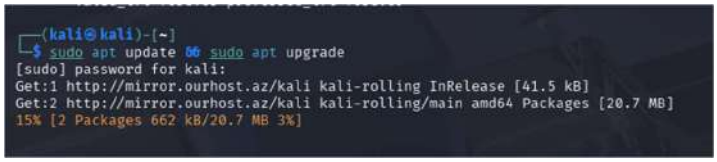
Run the command: **ip a**. We can see that the Kali VM has been assigned an IP address from the LAN network range. The VM should be able to access the internet as well.



Use the following command to update the system:

Sudo apt update && sudo apt get update

Enter password when prompted.



After the update is complete run the following command to remove the unused packages:

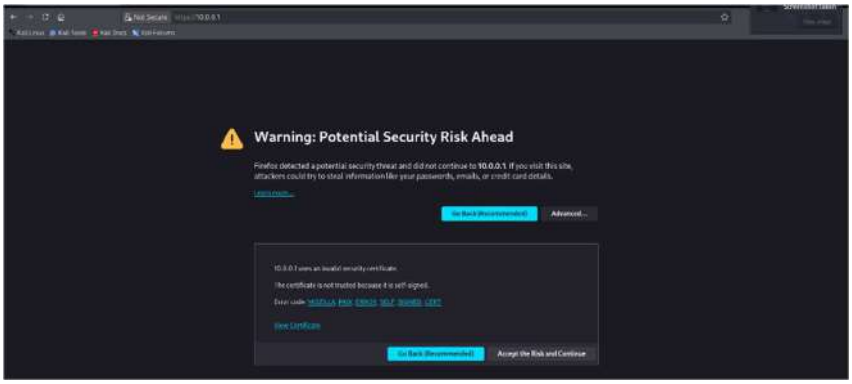
Sudo apt autoremove

On the Kali Linux VM, open the web browser and navigate to

https://10.0.0.1.

You will get the following message Warning: Potential Security Risk Ahead. This warning can be ignored. We get this warning because the URL that we are trying to access does not use the secure HTTP (HTTPS).

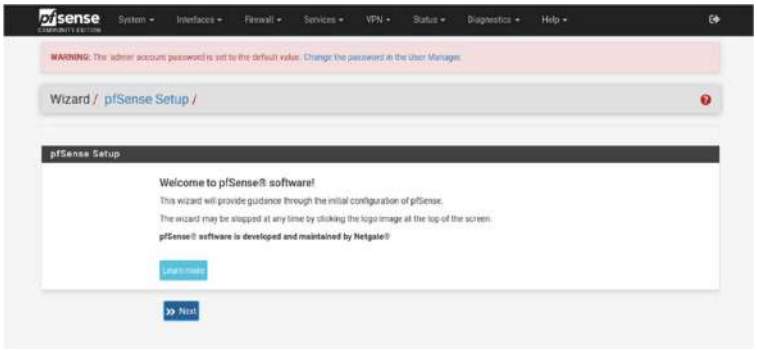
Click on **Advanced** and then click on **Accept the Risk and Continue**.



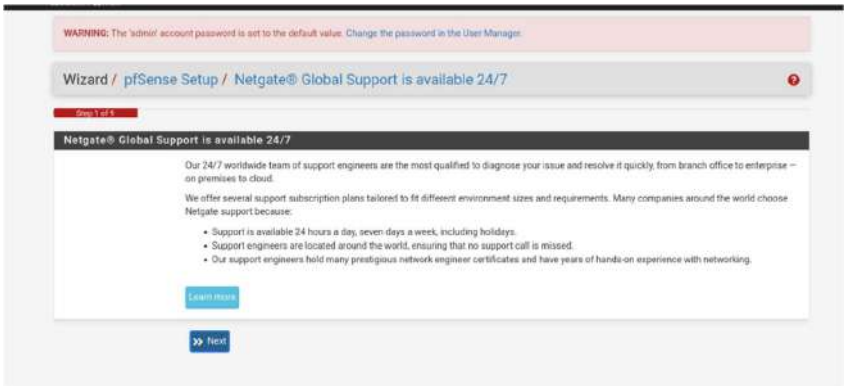
This will open the pfSense Web UI login page. Login using the default credentials.

Username: **admin**
Password: **pfsense**

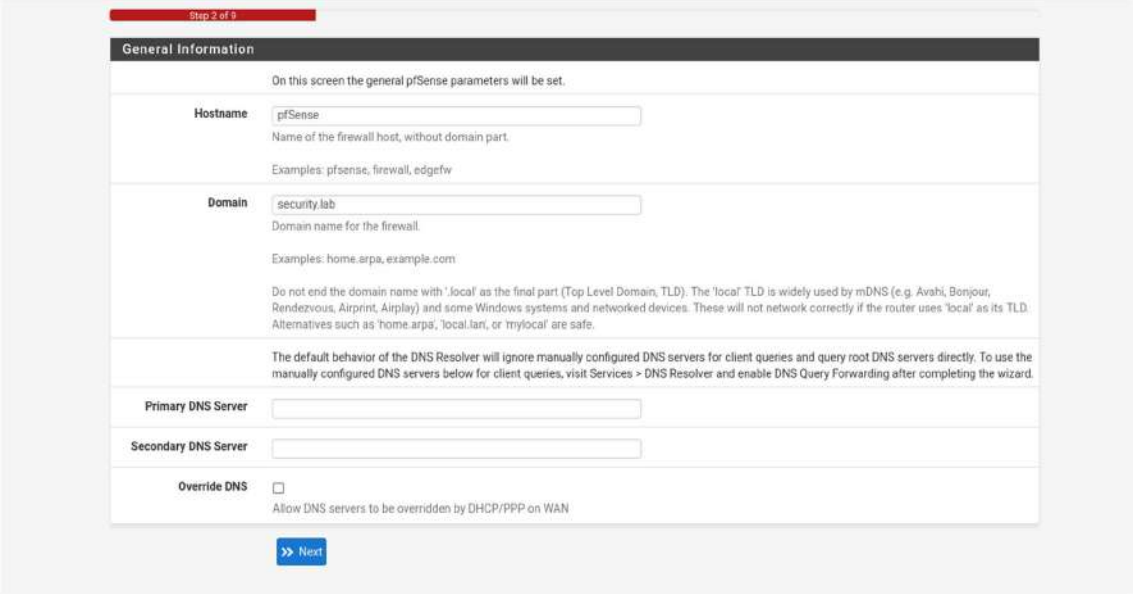
Click next



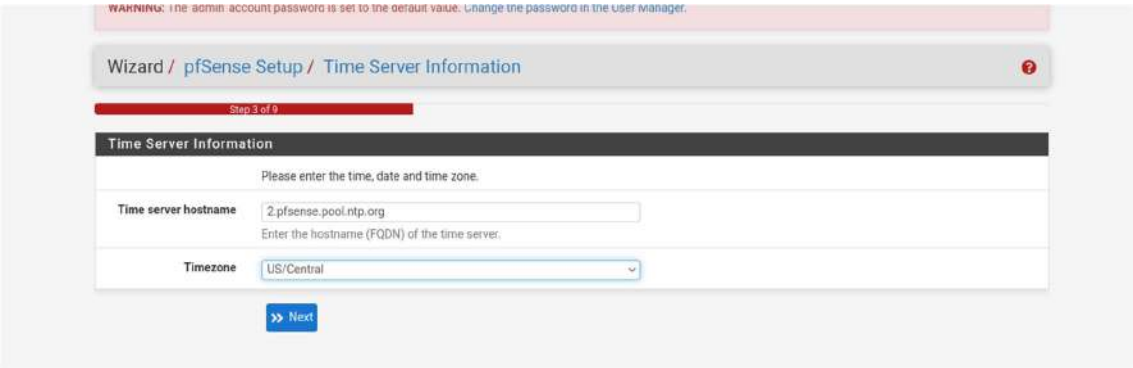
Click **Next** again.



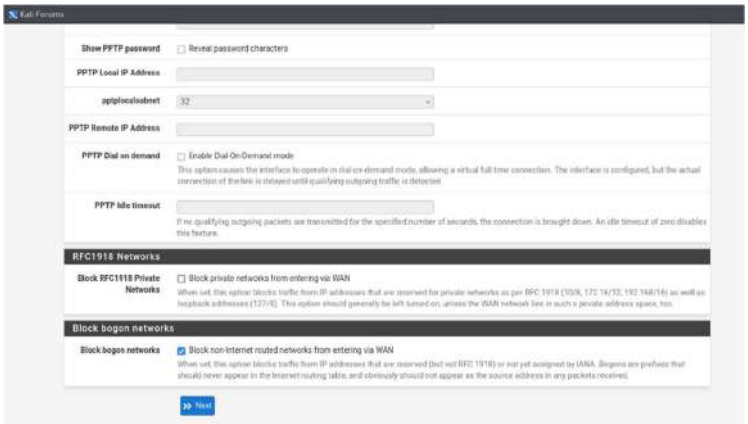
In the **General Information** section. Provide a Hostname and Domain name. This can be any name you choose. The hostname can be used to identify the pfSense VM on the network. Uncheck the Override DNS option and then click **Next**.



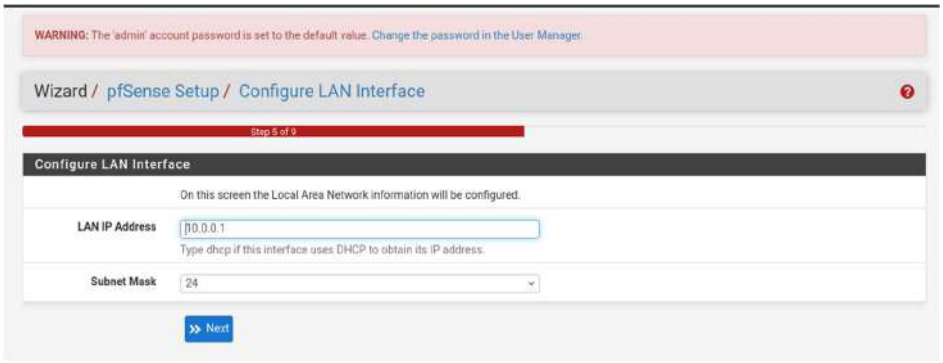
Select your Timezone and then click **Next**.



Scroll to the bottom of the page and look for the **RFC1918 Networks** section. Uncheck the Block RFC1918 Private Networks option.



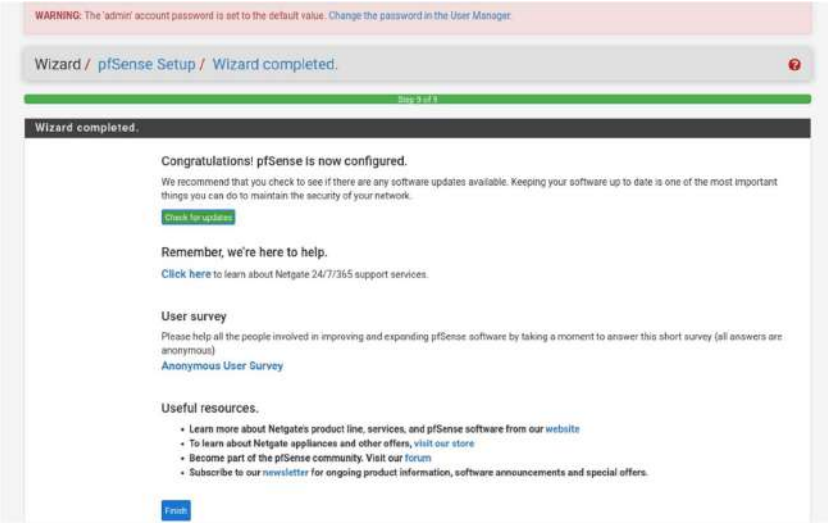
Don’t change any value on this page. Click on **Next**.



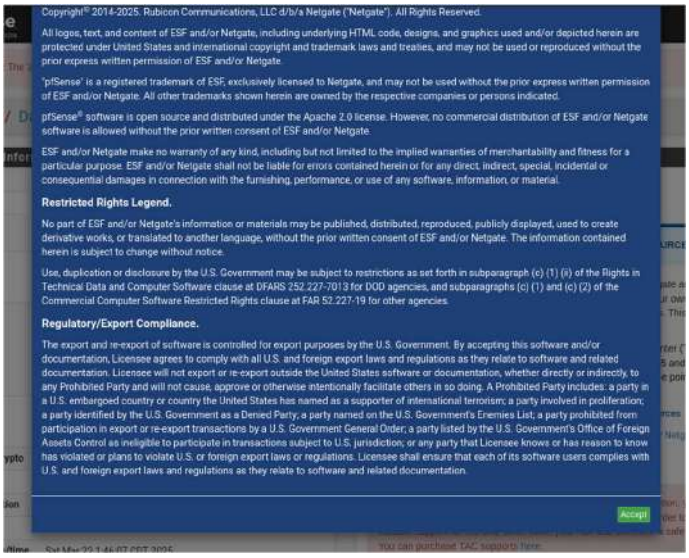
Enter a new password for the admin user. Store the password in a secure place.

Click on **Reload** to apply the changes.

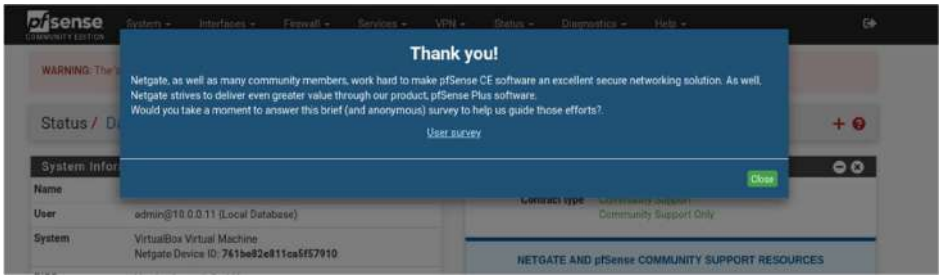
Click on **Finish**.



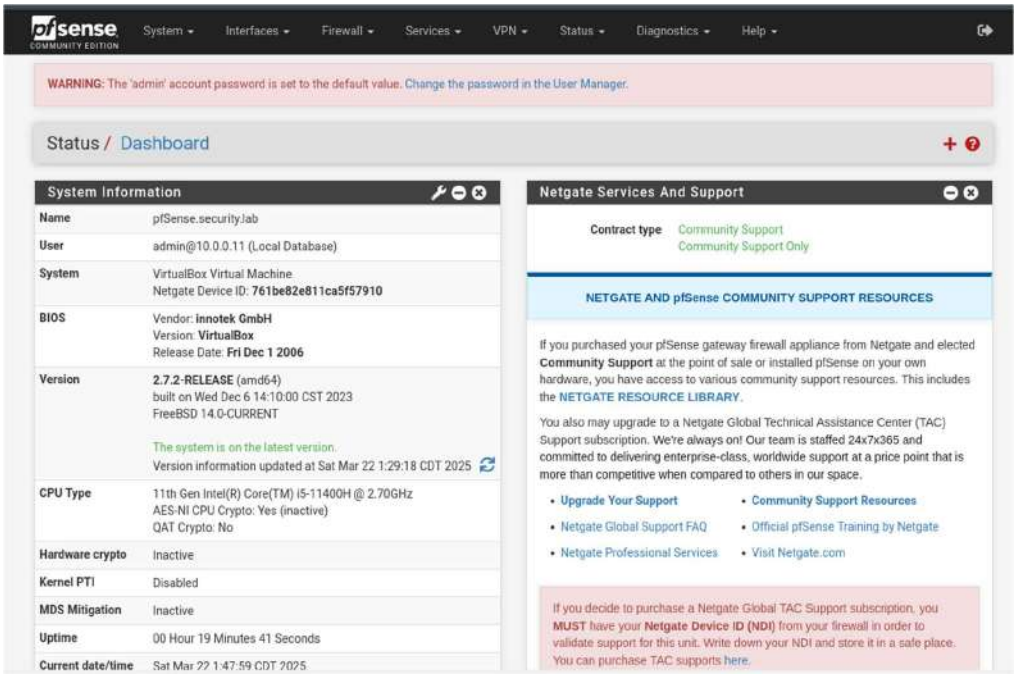
Click accept



Then click close

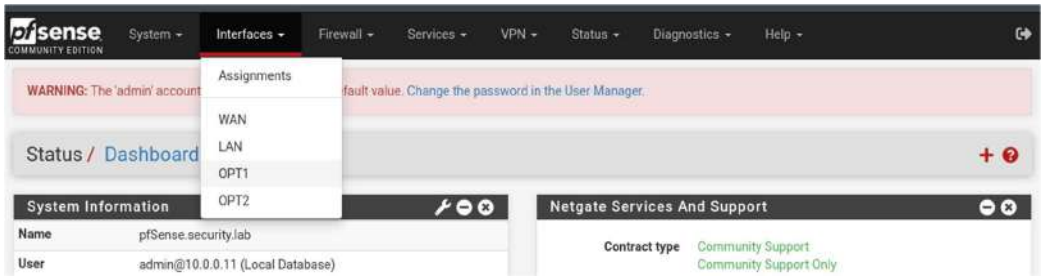


After interface looks like this

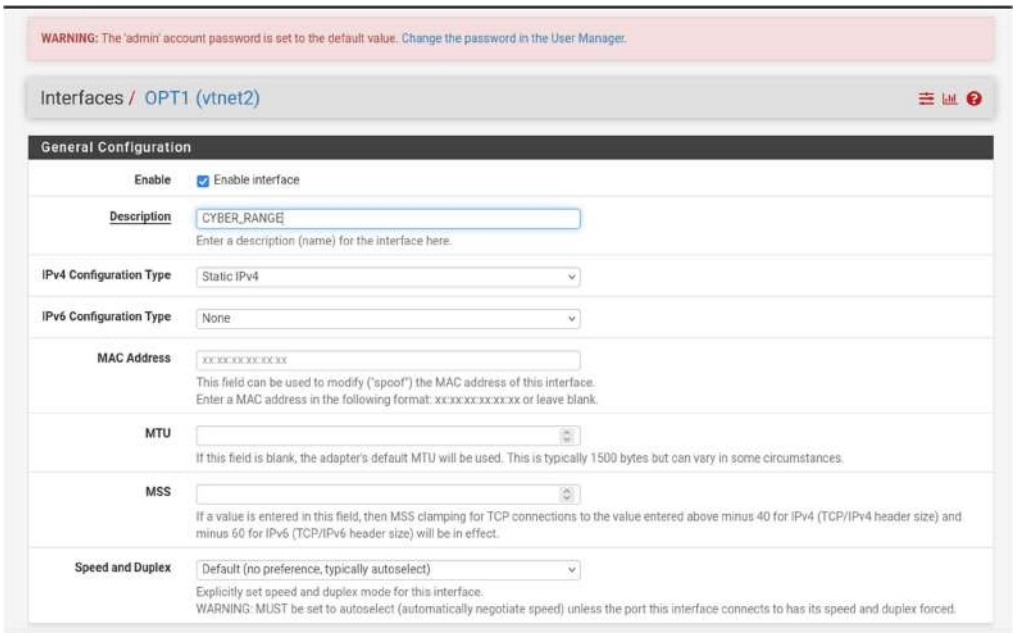


Interface Renaming

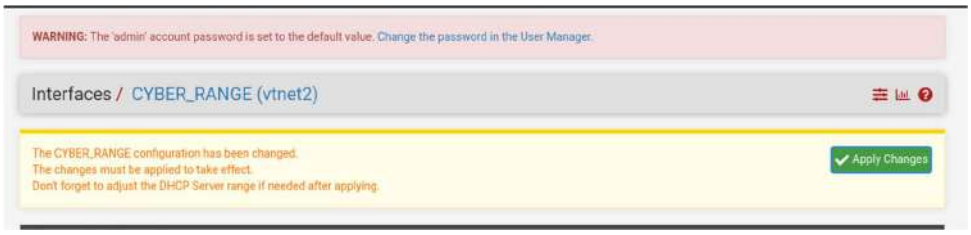
From the navigation bar select **Interfaces -> OPT1**.



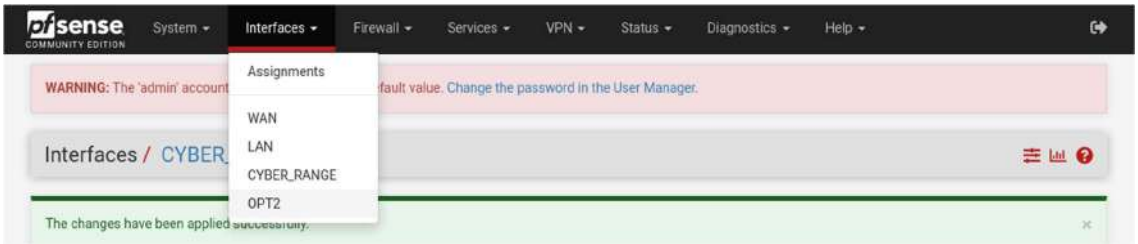
In the Description field enter **CYBER_RANGE**. Scroll to the bottom and click on **Save**.



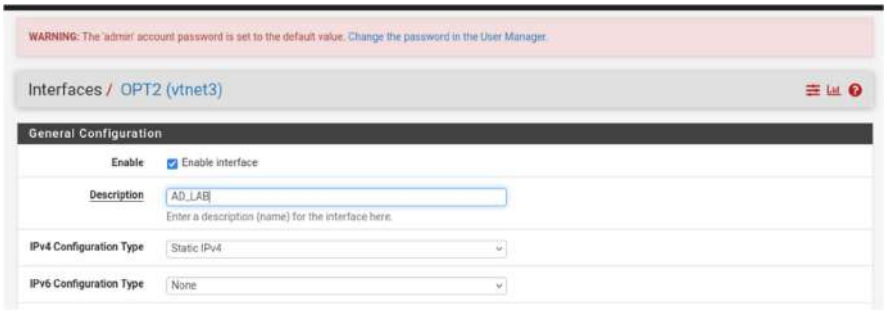
At the top of the page, a new popup will appear. Click on **Apply Changes**.



From the navigation bar select **Interfaces -> OPT2**.



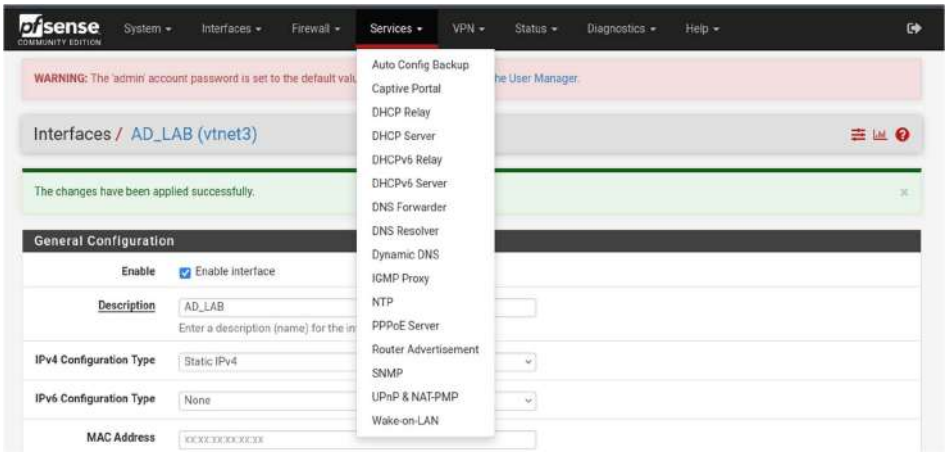
In the Description field enter **AD_LAB**. Scroll to the bottom of the page and click on **Save**.



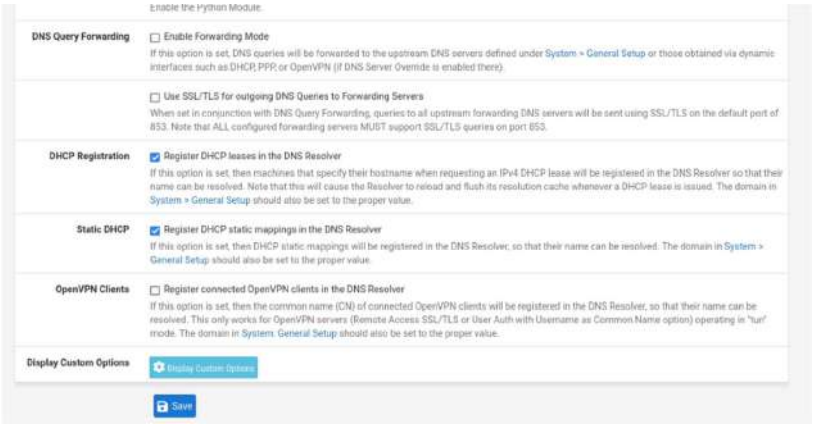
A popup will appear at the top of the page click on **Apply Changes**.

DNS Resolver Configuration

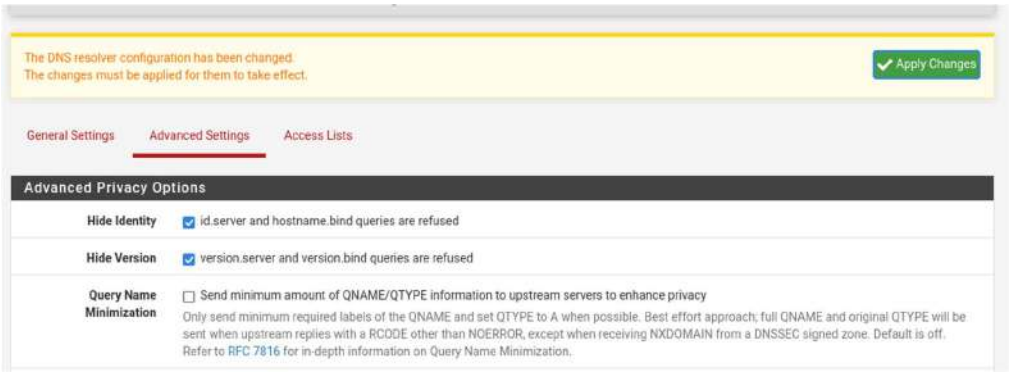
From the navigation bar select **Services -> DNS Resolver**.



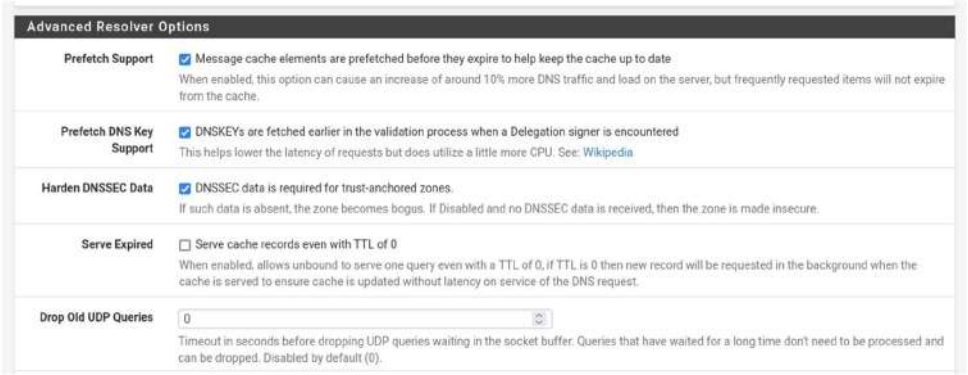
Scroll to the bottom of the page, look for the shown in image options and enable them. No need to save just yet. Scroll to the top of the page.



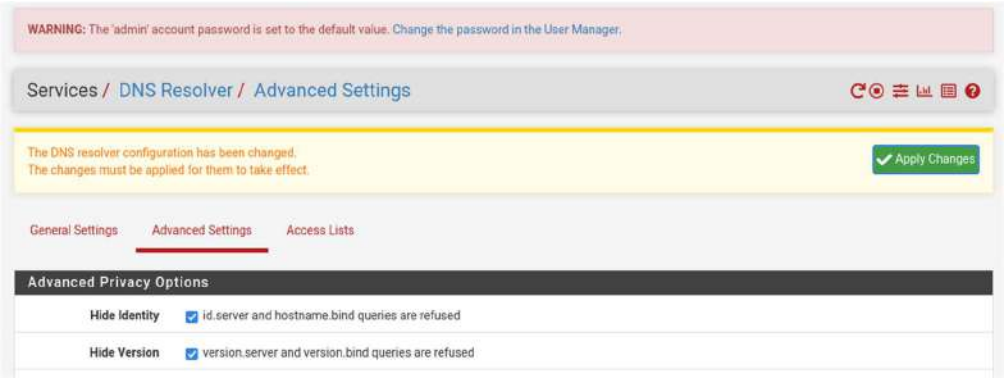
Click on **Advanced Settings**.



Scroll down to the **Advanced Resolver Options** section and enable the options shown in image. Scroll to the end and click on **Save**.



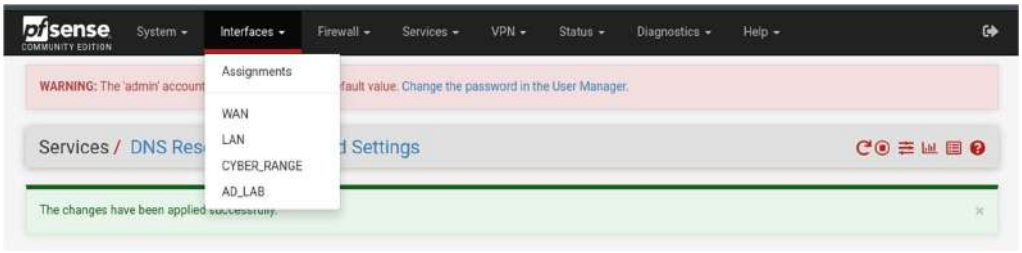
A popup will appear at the top of the page. Click on **Apply Changes**.



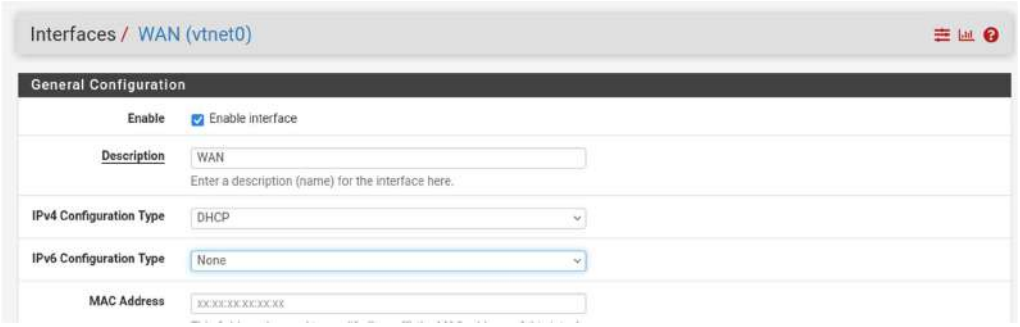
Disabling DHCPv6

Newer versions of VirtualBox/pfSense seem to prefer IPv6 for dynamic IP address assignment. You can disable DHCPv6 to prevent IPv6 addresses from being assigned to the WAN interface.

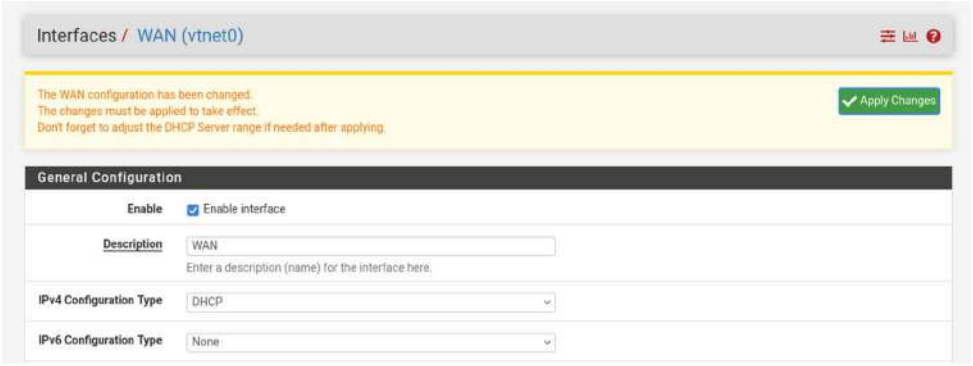
From the navigation bar select **Interfaces -> WAN**.



Set IPv6 Configuration Type to **None**. Scroll to the bottom and click on **Save**.



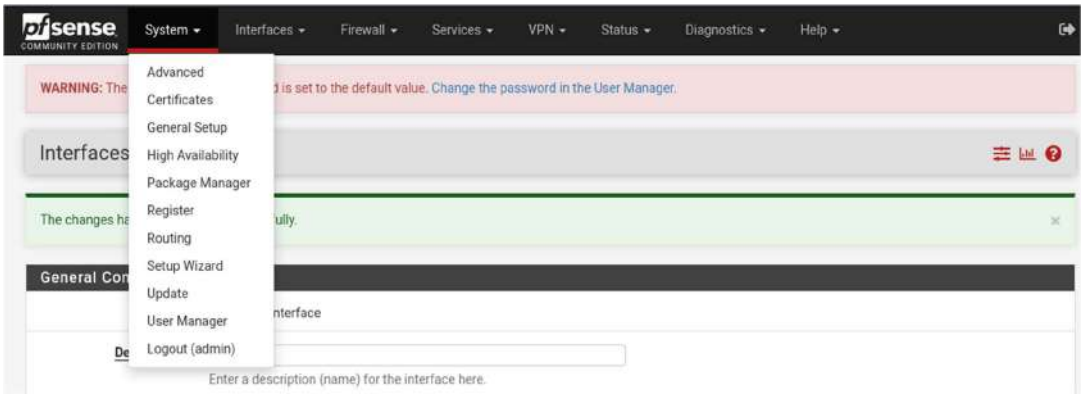
At the top of the page, a new popup will appear. Click on **Apply Changes**.



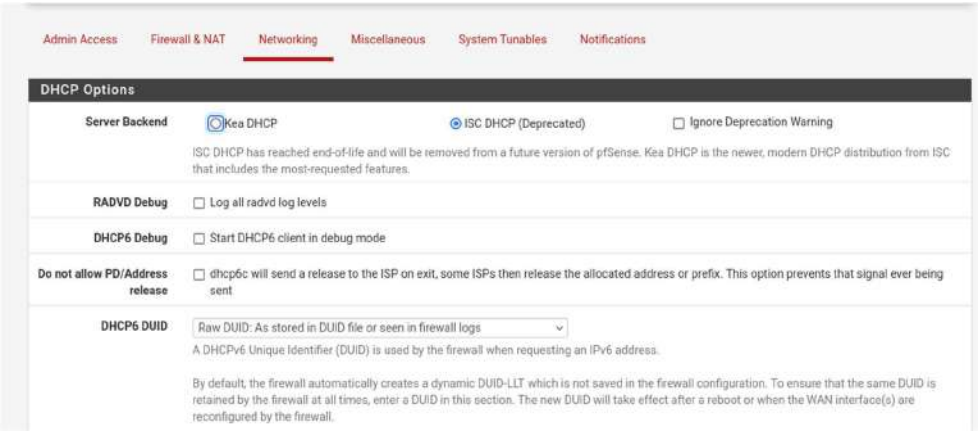
Restart the pfSense VM. Now, the WAN interface should have an IPv4 address.

Advanced Configuration

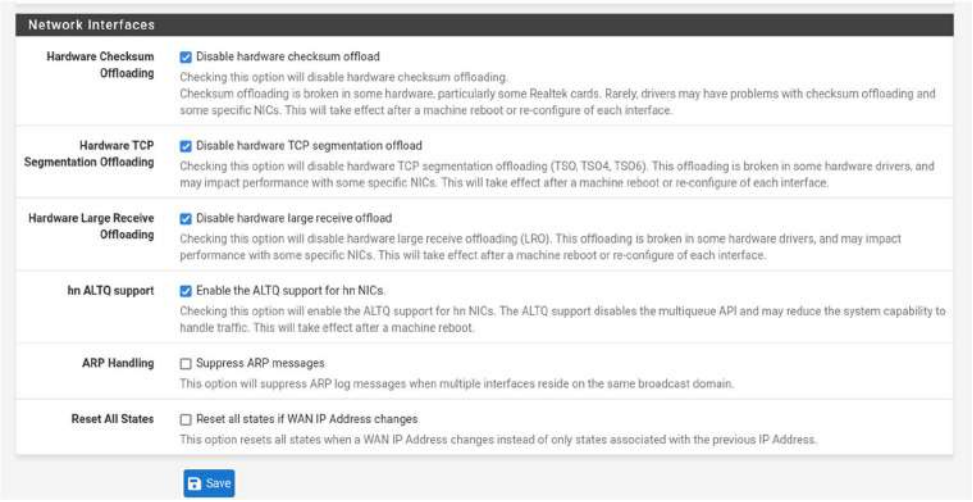
From the navigation bar select **System -> Advanced**.



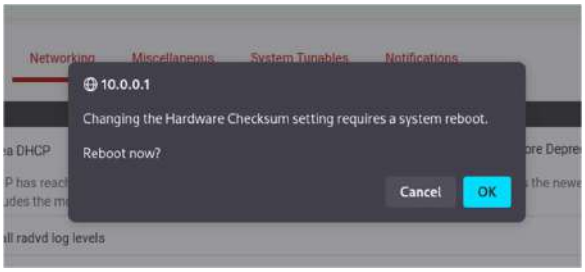
Go to the **Networking** tab



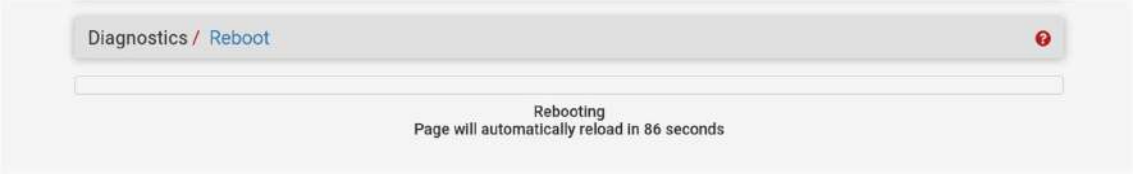
Scroll to the end in the **Network Interfaces** section and enable Disable hardware checksum offload. This option should improve the performance of pfSense. Click on **Save**.



A popup will appear click on **OK** to reboot pfSense.



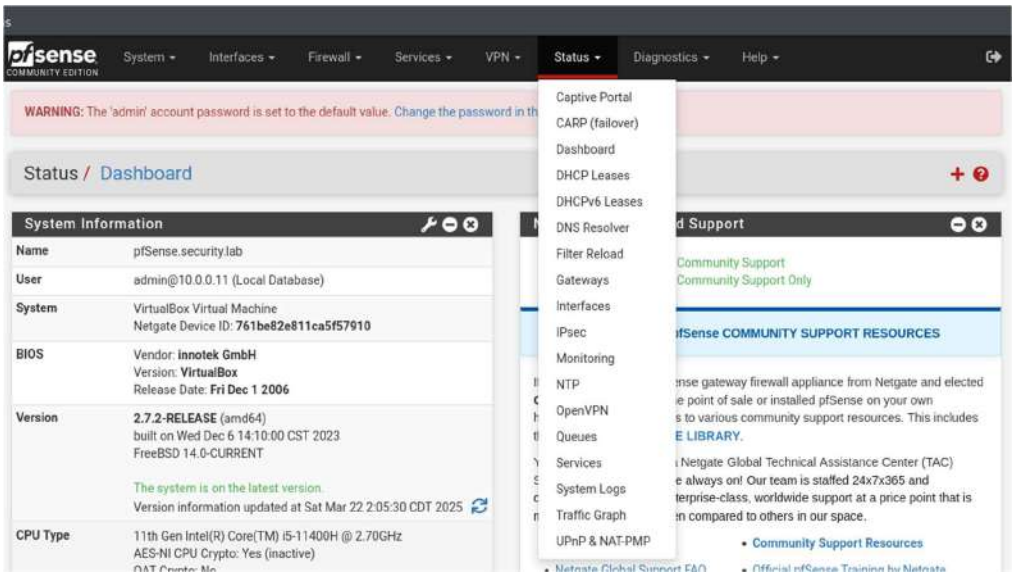
The following page will be shown while pfSense applies the changes.



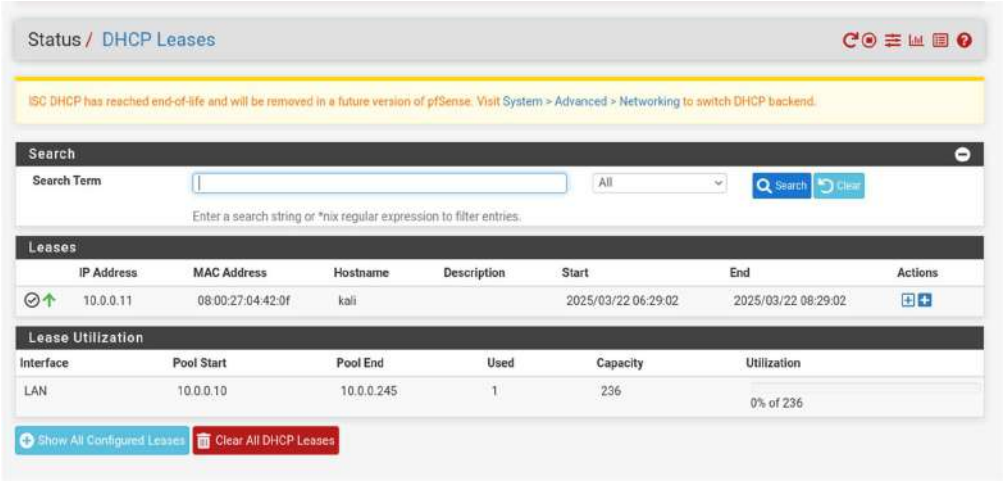
Once the reboot is complete we will be asked to log in again. Use the new password to access the Dashboard.

Kali Linux Static IP Assignment

From the navigation bar select **Status -> DHCP Leases**.

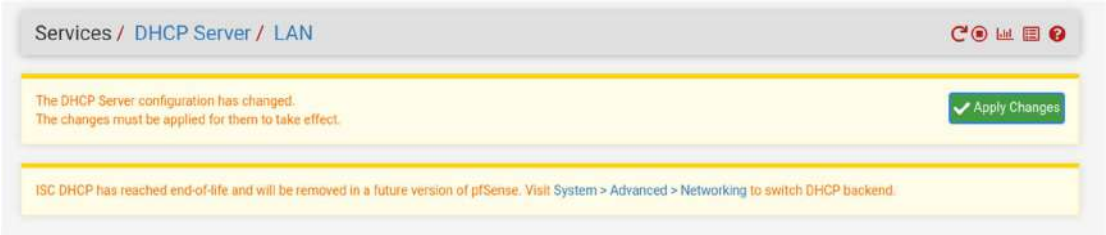


In the **Leases** section, we should see the Kali Linux VM with its current IP address. Click on + icon to assign a static IP to Kali Linux. The static IP will make it easier for us to apply firewall rules to interfaces that should only be able to reach the Kali VM.



In the IP Address input enter **10.0.0.2**. Scroll to the bottom and click on **Save**.

A popup will show up at the top of the page. Click on **Apply Changes**.



Refresh Kali Linux IP Address

Open a terminal on the VM. Use the following command to see the current IP address.

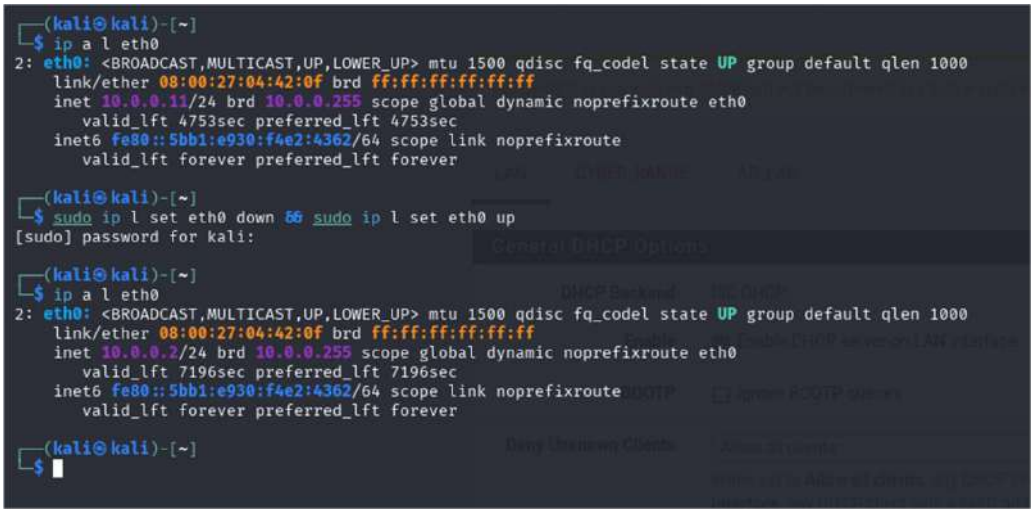
ip a l eth0

We want the VM to release the current IP address and use the static IP that was reserved. This can be achieved using the following command:

sudo ip l set eth0 down && sudo ip l set eth0 up

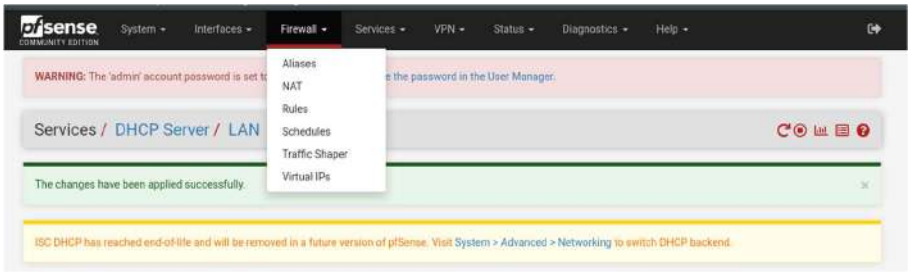
Enter password when prompted. To confirm that the VM is using the static IP run the following command:

ip a l eth0



pfSense Firewall Configuration

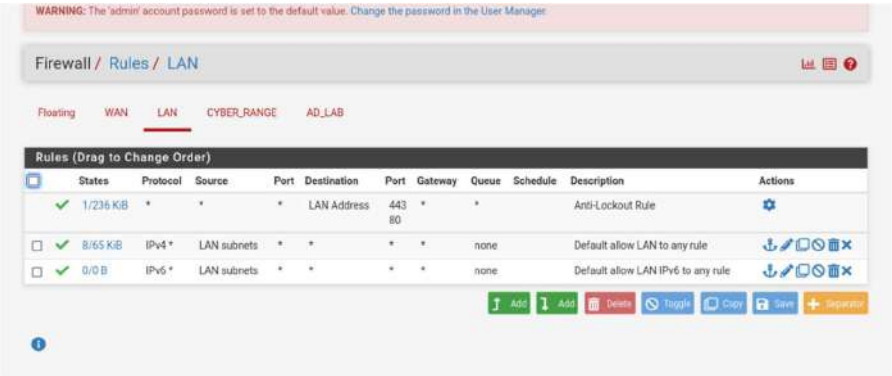
From the navigation bar select **Firewall -> Rules**.



LAN Rules

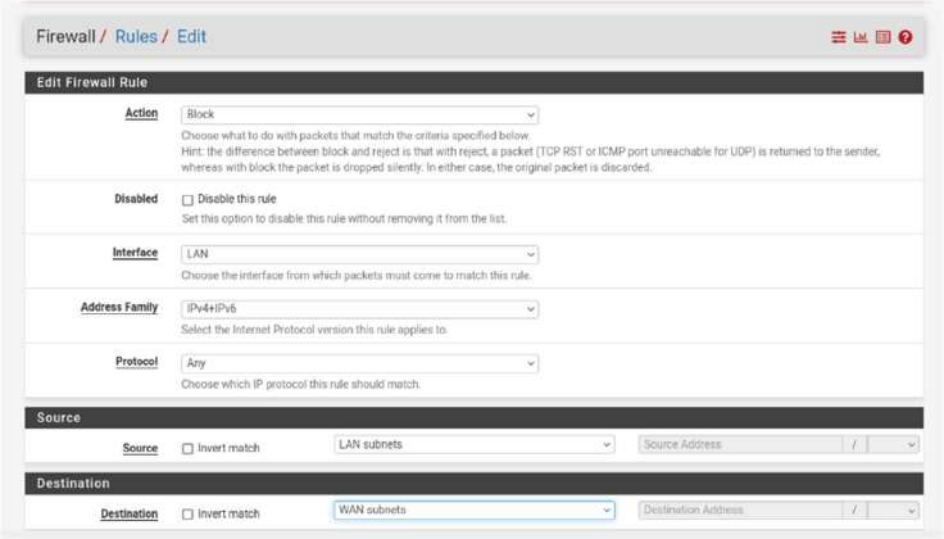
Go to the **LAN** tab. The LAN tab will have some predefined rules.

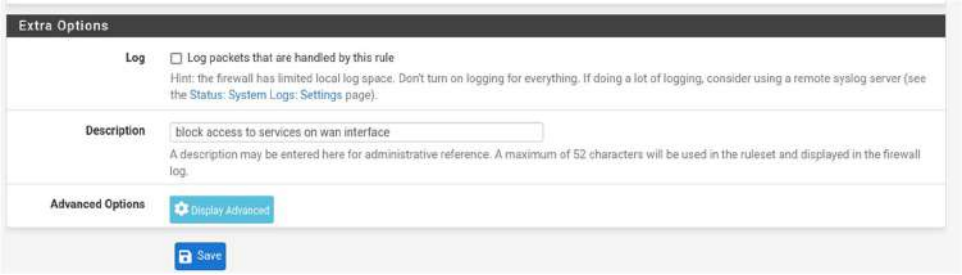
Click on the "Add rule to top" button to create a new rule.



Change the following options:
Action: **Block**
Address Family: **Ipv4+IPv6**
Protocol: **Any**
Source: **LAN subnets**
Destination: **WAN subnets**
Description: **Block access to services on WAN interface**

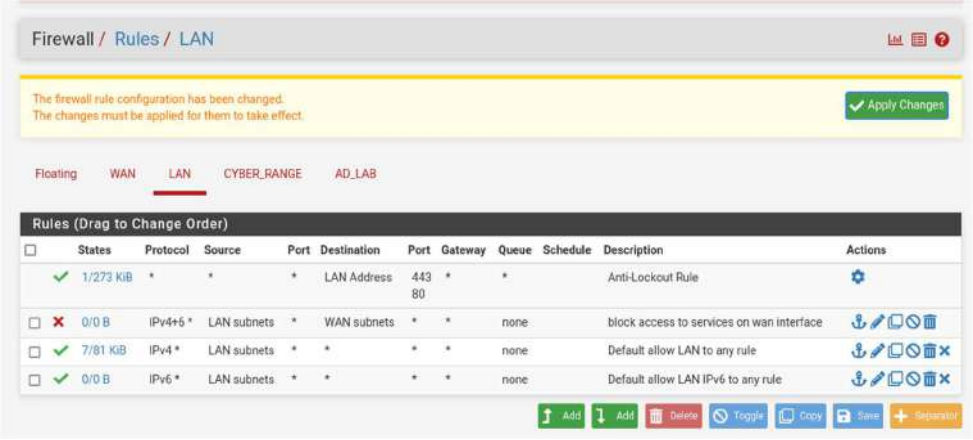
click on **Save**.





A popup will appear at the top of the page. Click on **Apply Changes**.

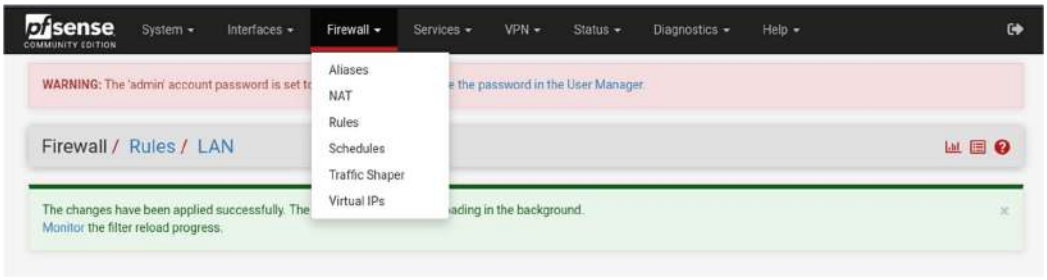
After that The final LAN rules should look as follows.



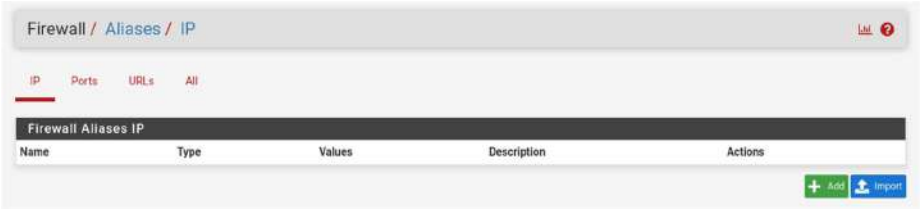
The order of the rules is important. If the order is not correct. Drag the rules around till it matches the above image.

CYBER_RANGE Rules

Before creating the rules for **CYBER_RANGE** we need to create a Alias. From the navigation bar select **Firewall -> Aliases**.

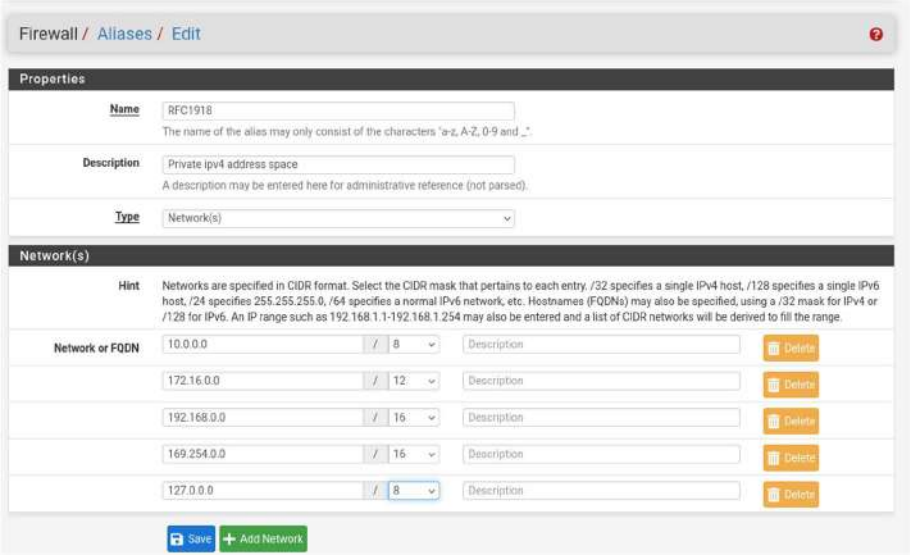


In the IP tab click on **Add** to create a new alias.



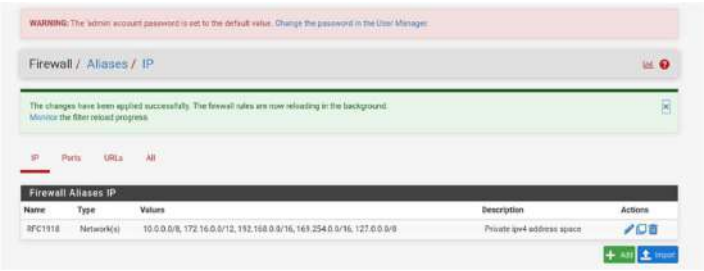
Enter the following details:
Name: **RFC1918**
Description: **Private IPv4 Address Space**
Type: **Network(s)**
Network 1: **10.0.0.0/8**
Network 2: **172.16.0.0/12**
Network 3: **192.168.0.0/16**
Network 4: **169.254.0.0/16**
Network 5: **127.0.0.0/8**

Click on **Save** to create an alias.

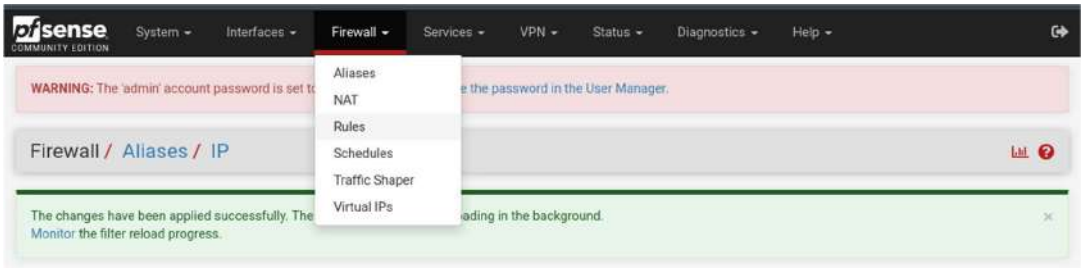


A popup will show up at the top click on **Apply Changes**.

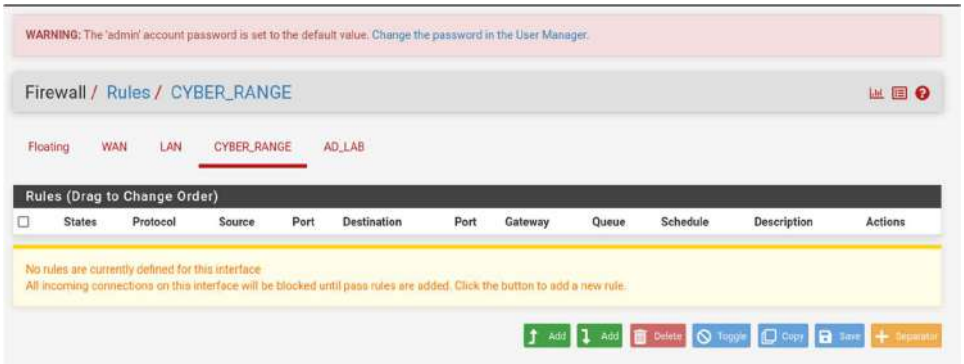
The final result should be as follows:



From the navigation bar select **Firewall -> Rules**.



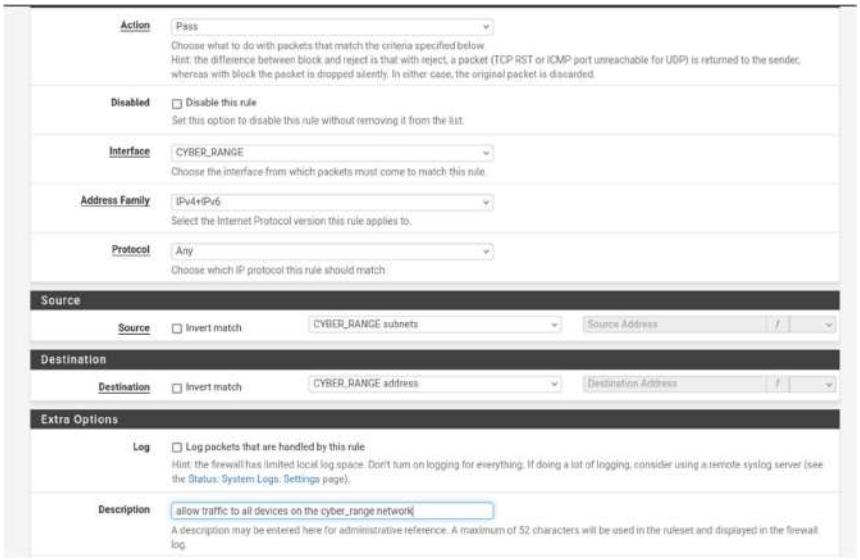
Select the **CYBER_RANGE** tab.



Use the "Add rule to end" button for all the rules.

Configure the rule as follows: Address Family: **IPv4+IPv6**
Protocol: **Any**
Source: **CYBER_RANGE subnets**
Destination: **CYBER_RANGE address**
Description: **Allow traffic to all devices on the CYBER_RANGE network**

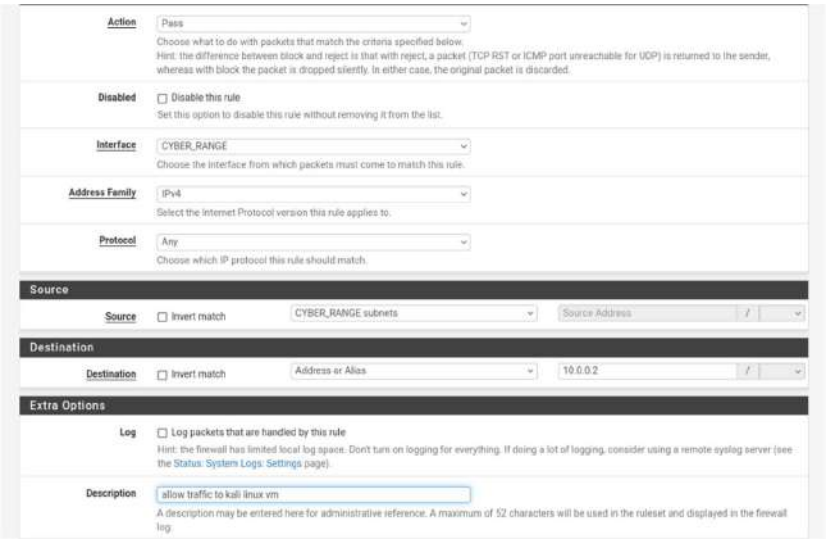
Scroll to the bottom and click on **Save**.



A popup will appear at the top to save the changes, no need to click on that just yet. Click on the "Add rule to end" button to create a new rule.

The rule has the following details:
Protocol: **Any**
Source: **CYBER_RANGE subnets**
Destination: **Address or Alias - 10.0.0.2**
Description: **Allow traffic to Kali Linux VM**

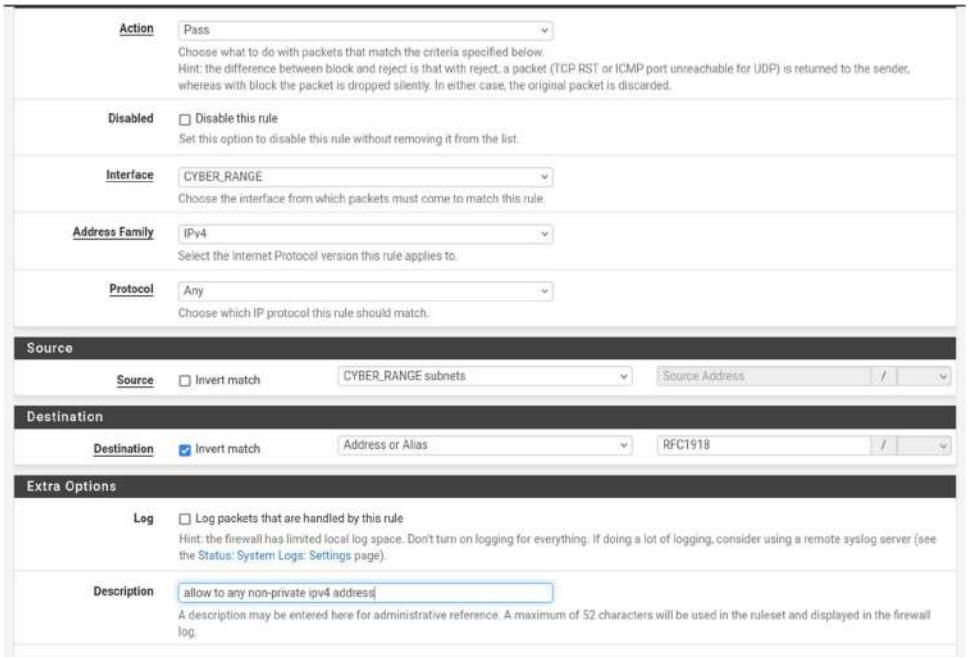
Scroll to the bottom and click on **Save**.



Click on the "Add rule to end" button to create a new rule.

Create a rule with the following settings:
Protocol: **Any**
Source: **CYBER_RANGE subnets**
Destination: **Address or Alias - RFC1918** (Select Invert match)
Description: **Allow to any non-private IPv4 Address**

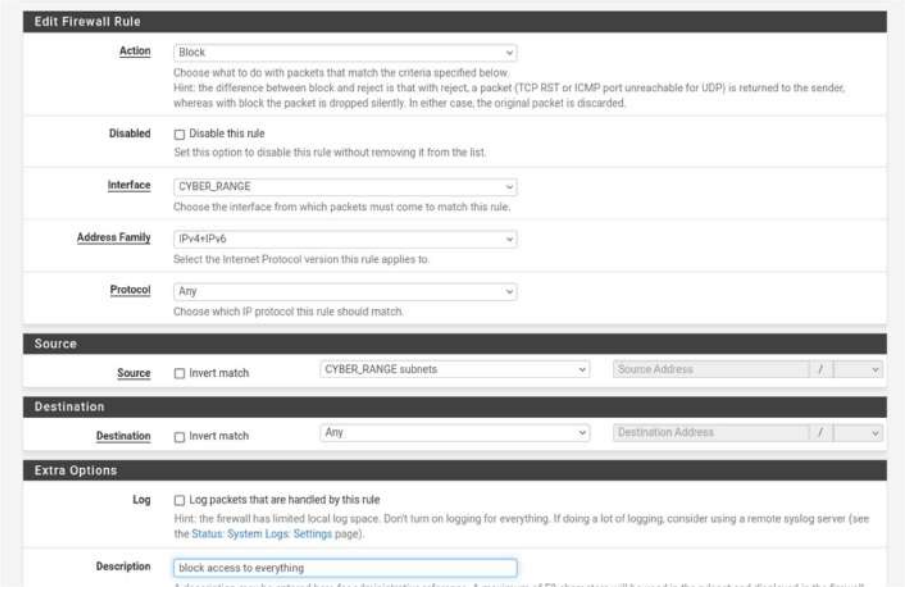
Scroll to the bottom and click on **Save**.



Click on the "Add rule to end" button to create a new rule.

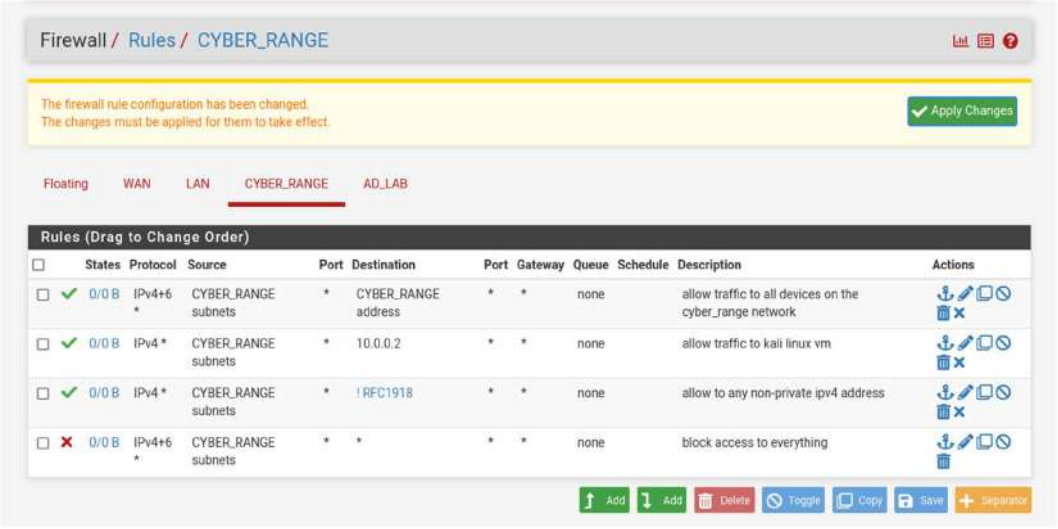
Create a rule with the following settings:
Action: **Block**
Address Family: **IPv4+IPv6**
Protocol: **Any**
Source: **CYBER_RANGE subnets**
Description: **Block access to everything**

Scroll to the bottom and click on **Save**.



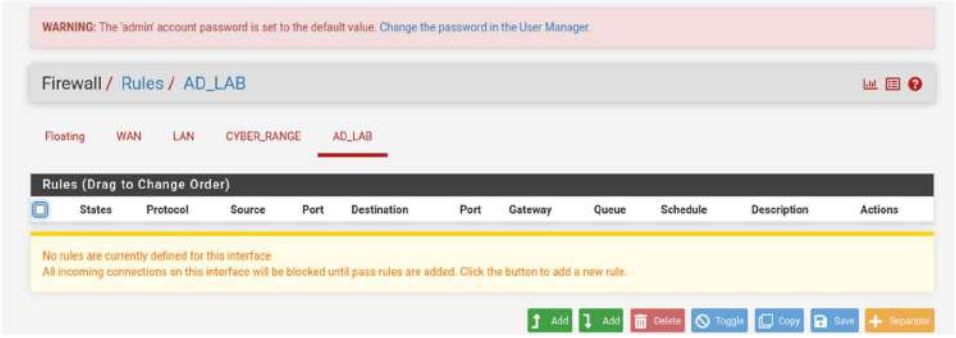
Click on the **Apply Changes** button in the popup at the top of the screen.

The final rules should look as follows:



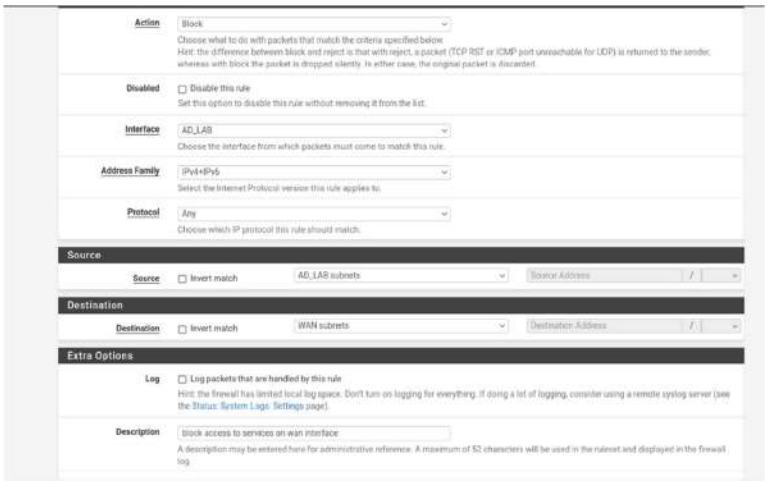
AD_LAB Rules

Click on the **AD_LAB** tab. Use the "Add rule to end" button to create new rules.



Create a rule with the following settings:
Action: **Block**
Address Family: **IPv4+IPv6**
Protocol: **Any**
Source: **AD_LAB subnets**
Destination: **WAN subnets**
Description: **Block access to services on WAN interface**

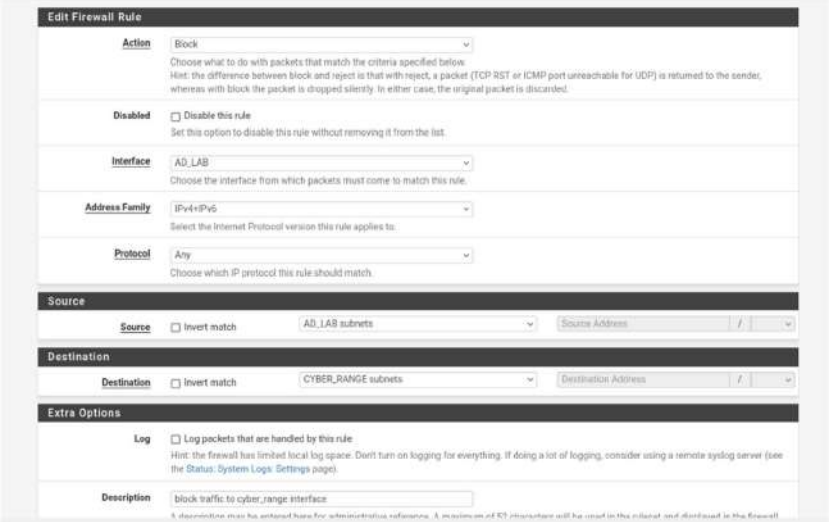
Scroll to the bottom and click on **Save**.



A popup will appear at the top to save the changes, no need to click on that just yet. Click on the "Add rule to end" button to create a new rule.

The rule has the following details:
Action: **Block**
Address Family: **IPv4+IPv6**
Protocol: **Any**
Source: **AD_LAB subnets**
Destination: **CYBER_RANGE subnets**
Description: **Block traffic to CYBER_RANGE interface**

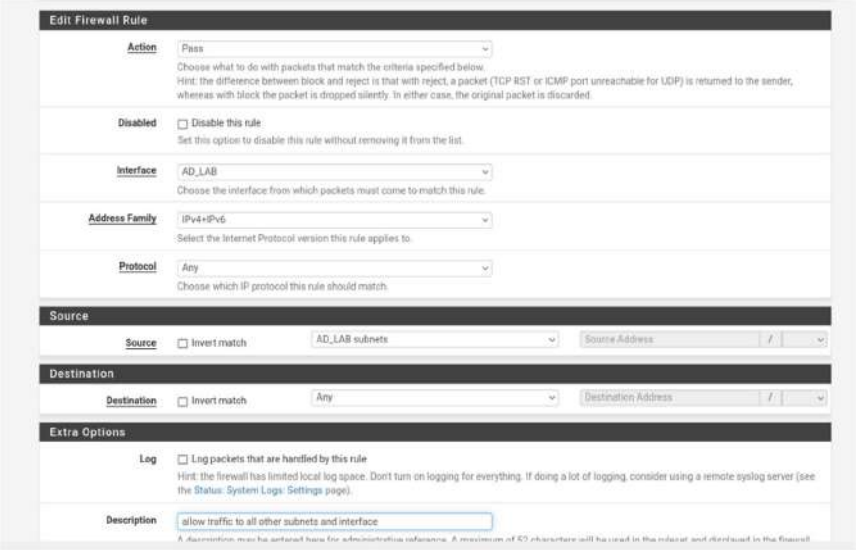
Scroll to the bottom and click on **Save**.



Click on the "Add rule to end" button to create a new rule.

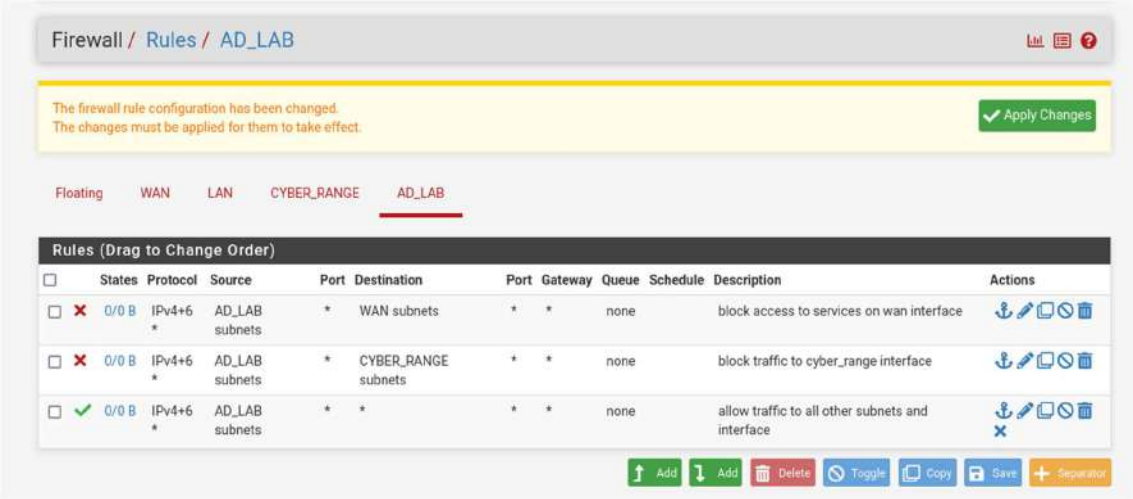
The rule has the following details:
Address Family: **IPv4+IPv6**
Protocol: **Any**
Source: **AD_LAB subnets**
Description: **Allow traffic to all other subnets and Internet**

Scroll to the bottom and click on **Save**.



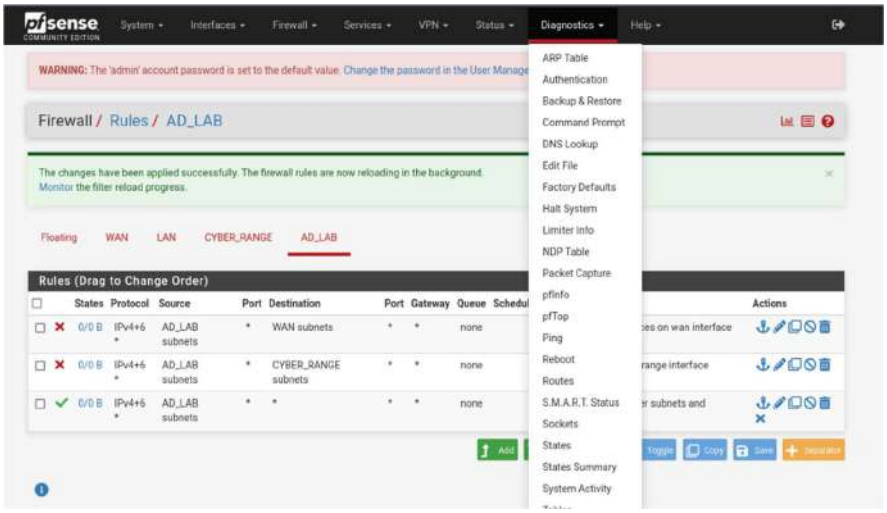
Click on the **Apply Changes** button in the popup at the top of the screen.

The final rules should look as follows:

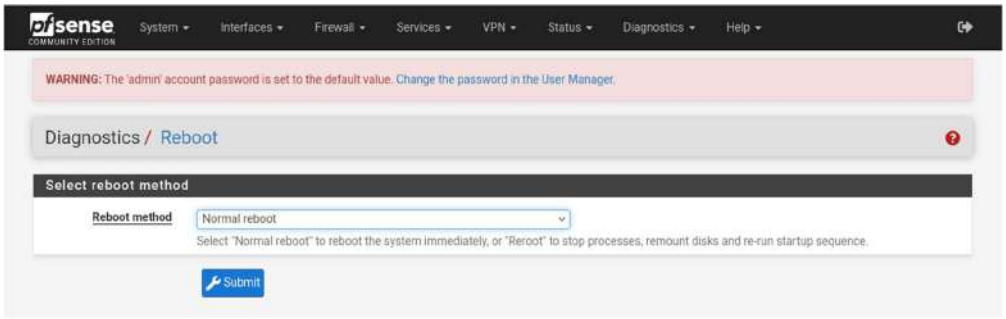


pfSense Reboot

Now we need to restart pfSense to persist the firewall rules. From the navigation bar select **Diagnostics -> Reboot**.



Click on **Submit**.



CYBER RANGE-Metasploit installation

Download Metasploitable 2

Go to the following URL: Metasploitable: 2 ~ VulnHub and download Metasploitable.

The download is a compressed file (**.zip**). Use an extraction software like **7-zip** to decompress the file. After extraction, we should have a folder.

Creating the VM

Launch VirtualBox. Select Tools from the sidebar, then click on **New** from the toolbar.

Give the VM a name. Ensure that the Folder is set to the location where all the VMs of the Home Lab are going to be saved. Leave the ISO Image option empty. Select the value for Type and Version as shown below and then click on **Next**.

Reduce the Memory to **1024MB** and click on **Next**.

Select "Do Not Add a Virtual Hard Disk" and click on **Next**.

Confirm that everything looks correct and click on **Finish**.

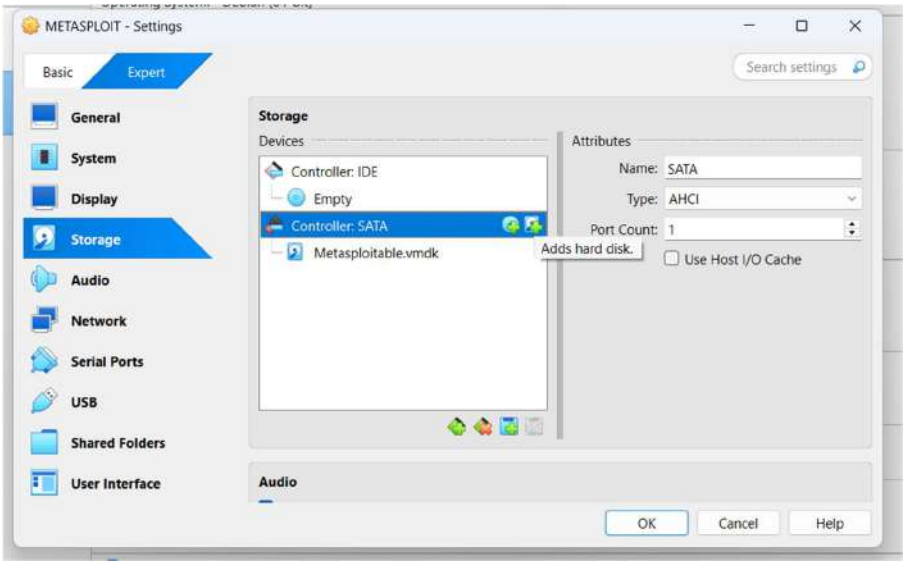
Ll my VMs for the Home Lab project are located in **D:\Virtual Machines**. Whenever we create a new group in VirtualBox a corresponding folder is created is created on the filesystem to store the VM.

Since the Metasploitable 2 VM is in the Cyber Range group which is nested inside the Home Lab group the location of the Metasploitable VM on my Hard Drive will be **D:\Virtual Machines\Home Lab\Cyber Range\Metasploitable 2**.

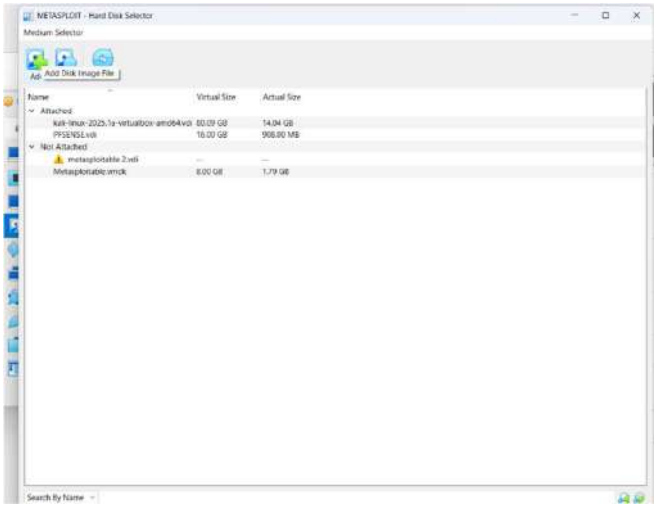
Find the Metasploitable VM folder location in your case and move the downloaded **.vmdk** into it.

Select the VM from the sidebar and then from the toolbar click on **Settings**.

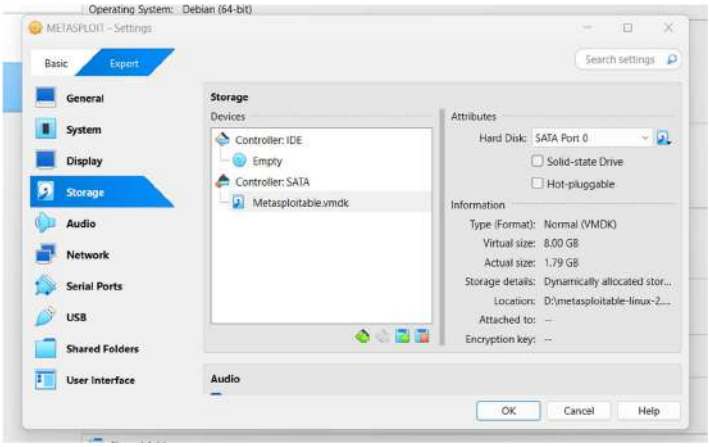
Go to **Storage** and select **Controller: SATA** then click on the small "Add Hard Disk" icon on the right.



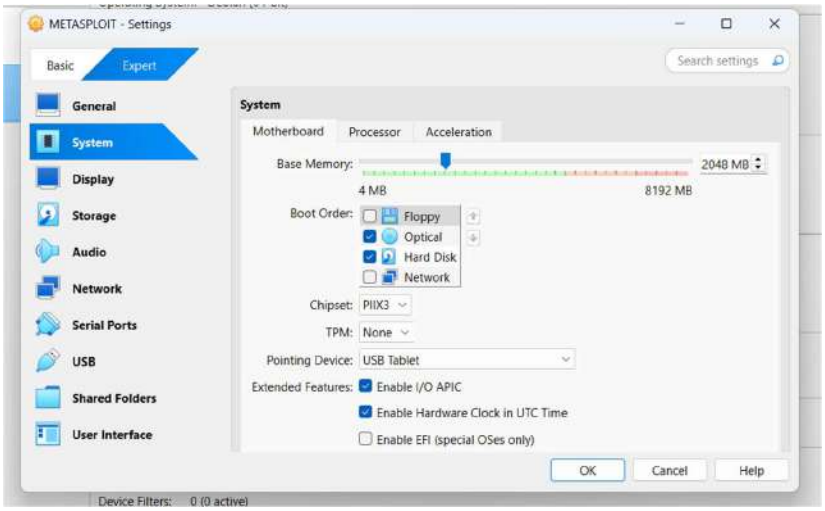
This will open the Hard Disk Selector menu. Click on Add and then select the **.vmdk** file. Then click on the Choose button to use the Hard Drive.



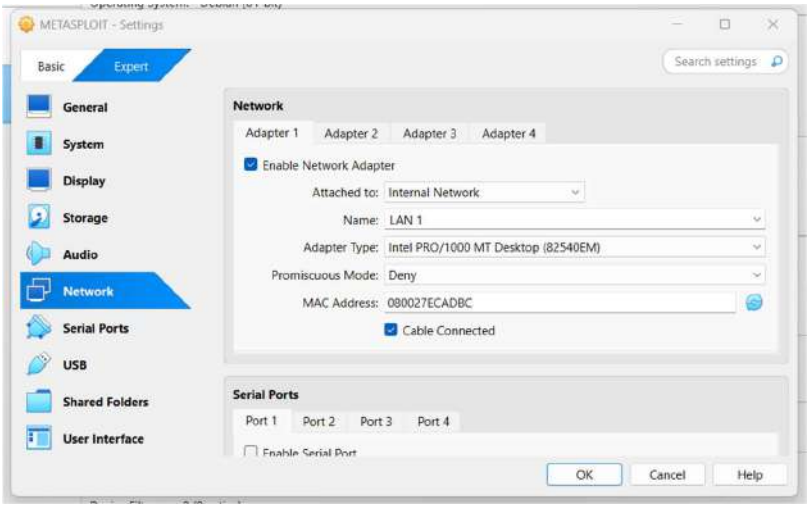
If done correctly under **Controller: SATA** the Hard Disk will be visible.



Go to **System -> Motherboard**. For Boot Order ensure that the **Hard Disk** is on the top followed by **Optical**. Disable **Floppy**.



Go to **Network -> Adapter 1**. Change the Attacked to field to **Internal Network** and in Name select **LAN 1**. Click on **OK** to save the changes.



From the sidebar select Metasploitable 2 and then click on **Start**.

Once the VM boots use the following credentials to log in.
Username: **msfadmin**
Password: **msfadmin**

After login use the following command to check if we have an IP address:

ip a l eth0

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:ec:ad:bc brd ff:ff:ff:ff:ff:ff
    inet 10.6.6.11/24 brd 10.6.6.255 scope global eth0
    inet6 fe80::a00:27ff:feec:adbc/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

We can ping Google to test if we have an Internet connection.

Ping google.com

```
msfadmin@metasploitable:~$ ping google.com
PING google.com (142.251.42.46) 56(84) bytes of data.
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=1 ttl=254 time
=45.5 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=2 ttl=254 time
=55.4 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=3 ttl=254 time
=44.0 ms
64 bytes from bom12s20-in-f14.1e100.net (142.251.42.46): icmp_seq=4 ttl=254 time
=42.0 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3942ms
rtt min/avg/max/mdev = 42.032/46.787/55.483/5.179 ms
```

We can do a similar test to check connectivity to the Kali Linux.

Ping 10.0.0.2

```
msfadmin@metasploitable:~$ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=63 time=6.72 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=63 time=3.09 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=63 time=2.85 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=63 time=2.48 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=63 time=2.08 ms

--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 2.083/3.448/6.724/1.673 ms
msfadmin@metasploitable:~$
```

ACTIVE DIRECTORY SETUP

Windows Server 2019

Go to the following URL: Windows Server 2019 | Microsoft Evaluation Center

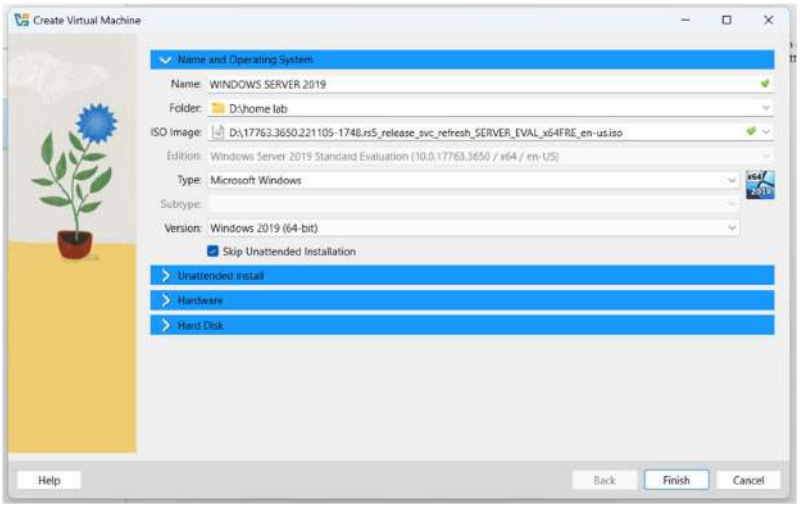
Click on the **64-bit edition** download. The ISO file is ~5GB.

Creating the VM

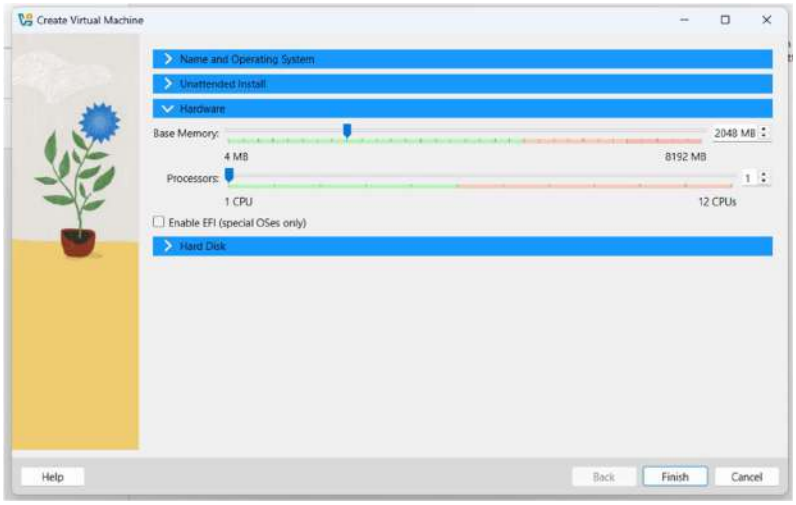
Windows Server 2019

Click on Tools from the VirtualBox sidebar and select **New**

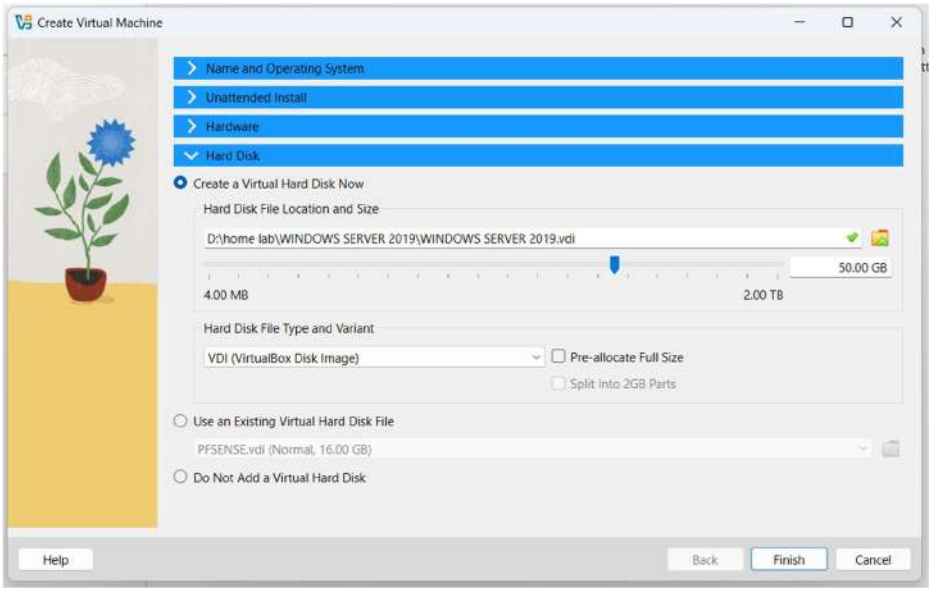
Gave the VM a name. Ensure that the Folder option points to the location where all the Home Lab-related VMs are saved. For the ISO Image select the downloaded Windows Server 2019 image. Select the **Skip Unattended Installation** option and then click on **Next**.



Increase the Memory to 2048MB (2GB) and click on Next.



Increase the Hard Drive size to **50GB** and then click on **FINISH**.

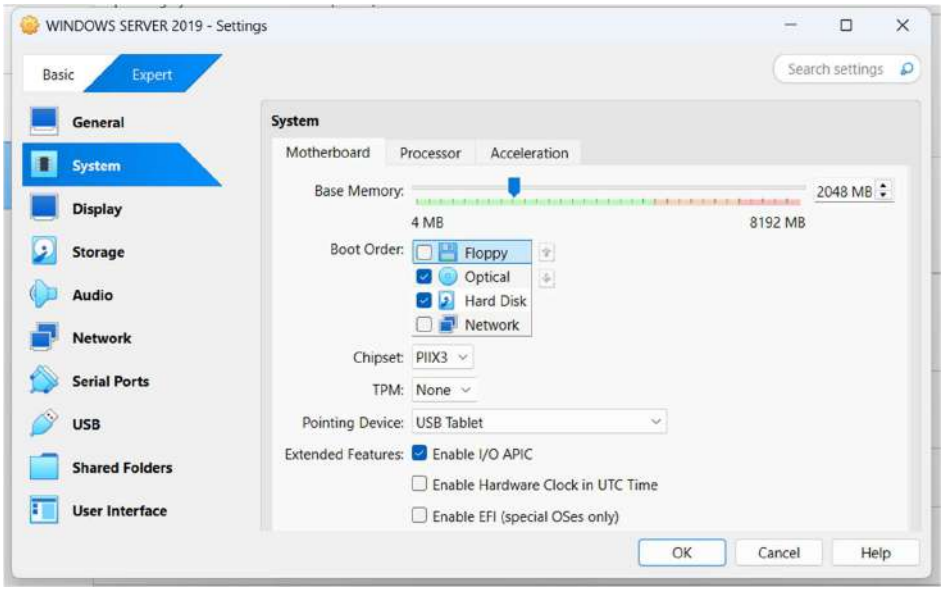


Configuring the VM

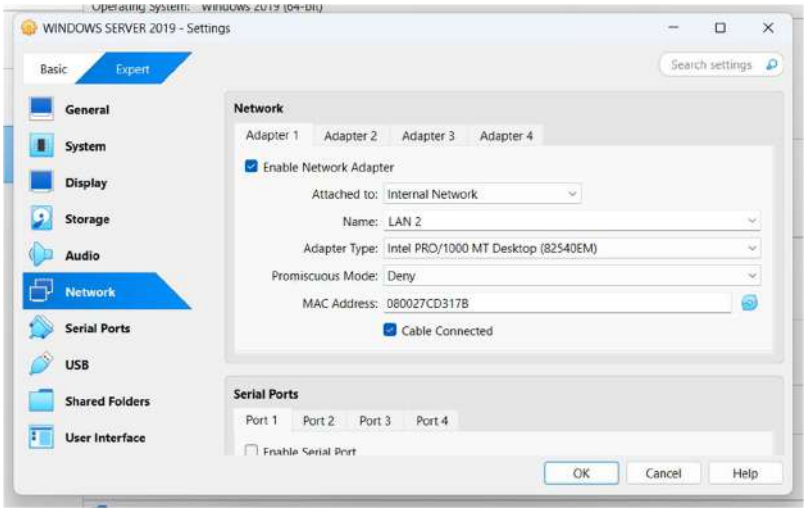
Windows Server 2019

Select the Windows Server 2019 VM and click on Settings from the toolbar.

Go to **System -> Motherboard**. For Boot Order ensure **Hard Disk** is not the top followed by **Optical**. Disable **Floppy**.



Go to **Network -> Adapter 1**. For the Attacked to field select **Internal Network**.
For name select **LAN 2**. Click on **OK** to save the settings.

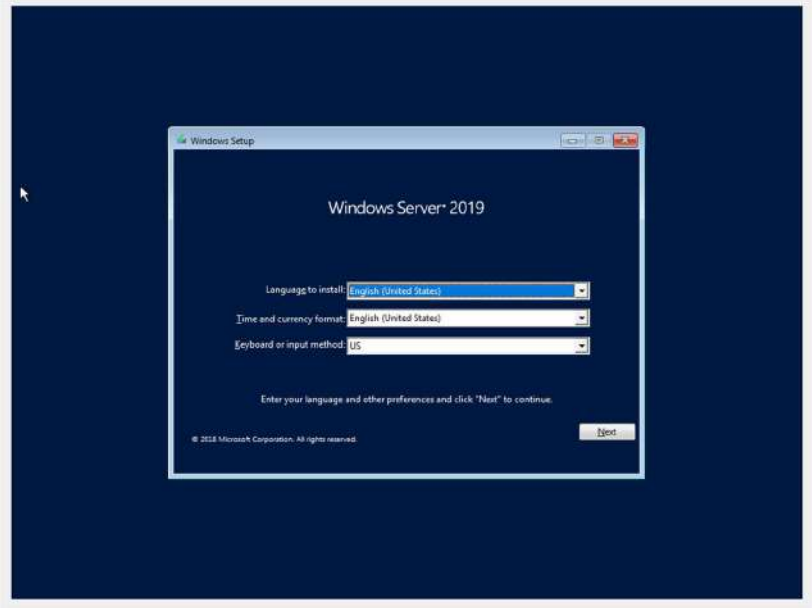


Windows Server 2019 Setup

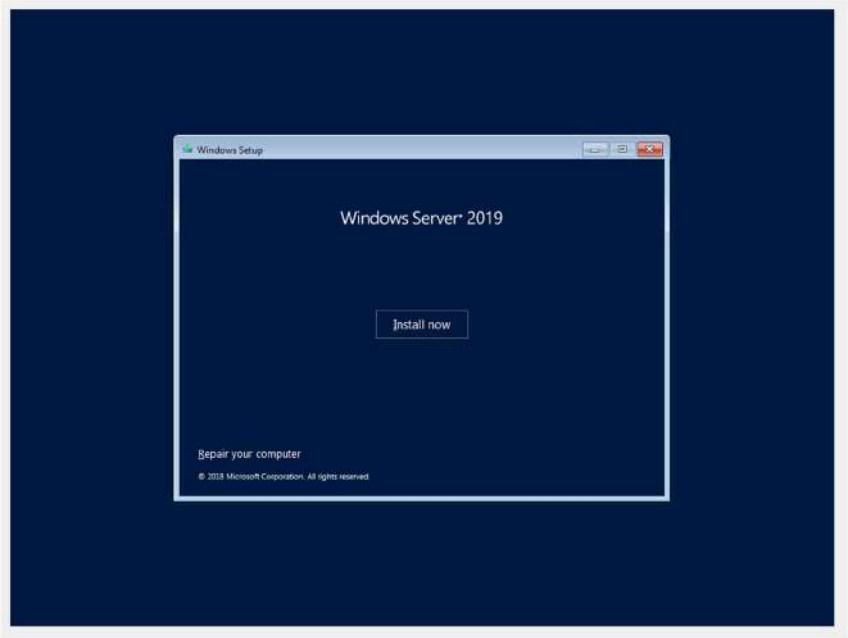
OS Installation

Select Windows Server 2019 from the sidebar and click on **Start** from the toolbar.

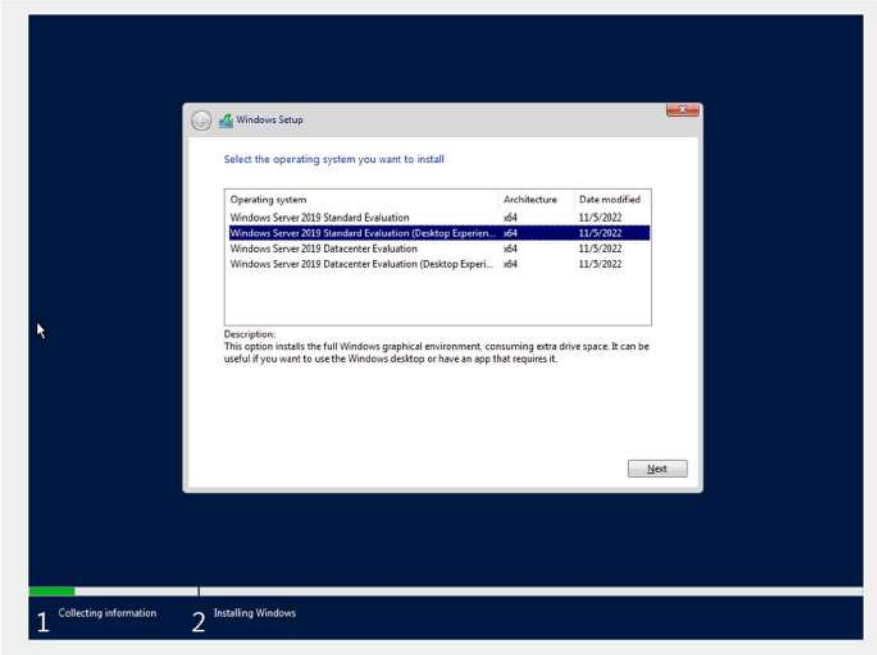
Click on **Next**.



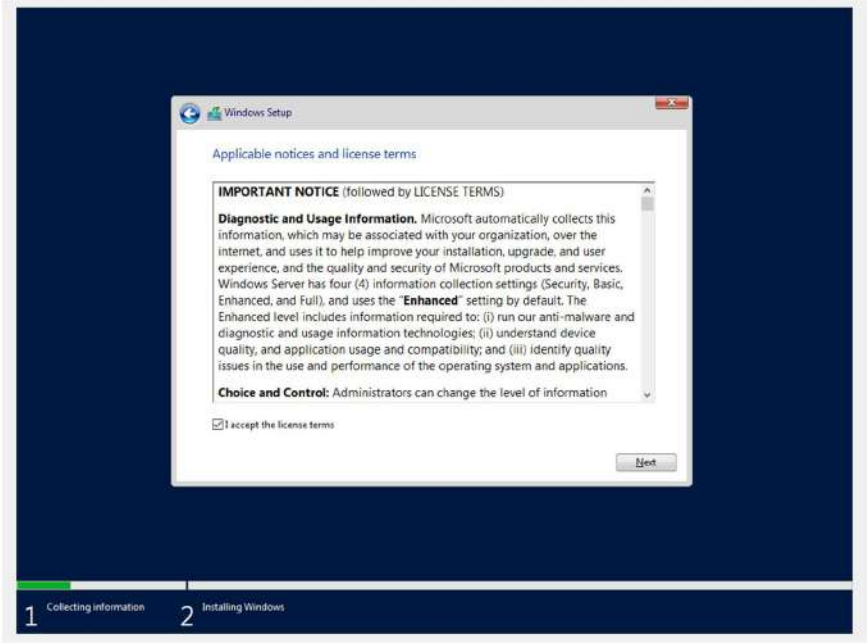
Click on **Install now**.



Select **Windows Server 2019 Standalone Evaluation (Desktop Experience)** and click on **Next**.

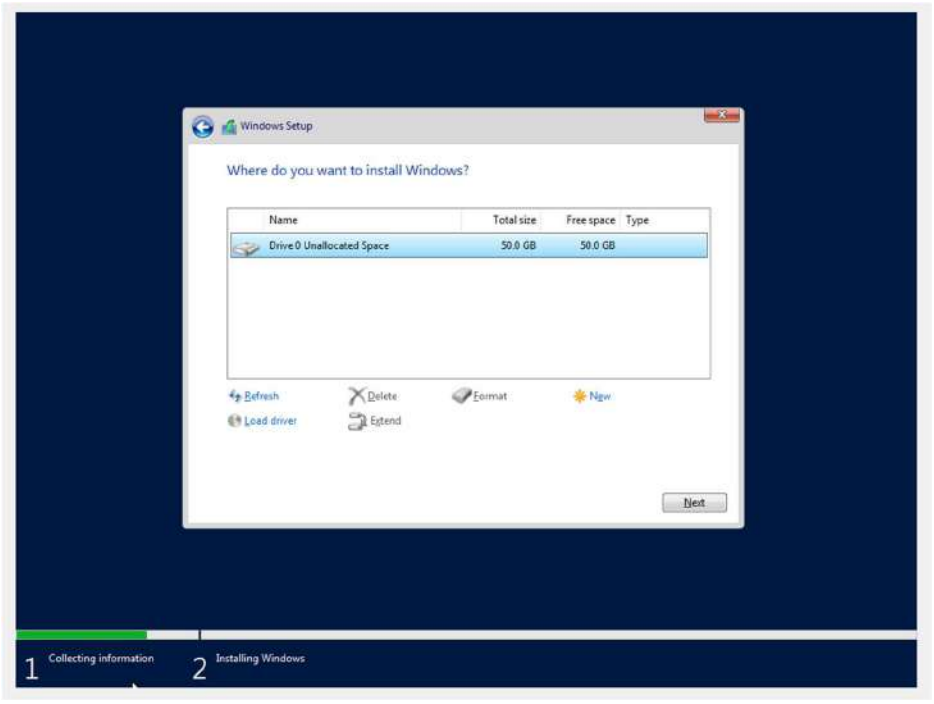


Accept the agreement and click on **Next**.

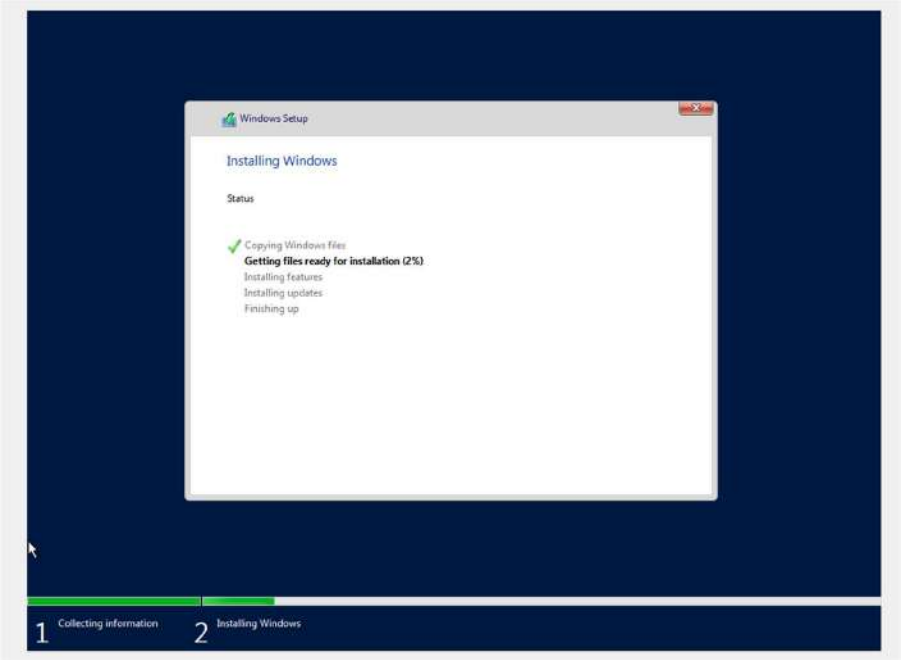


Select **Custom: Install Windows only (Advanced)**.

Select **Disk 0** and click on **Next**.

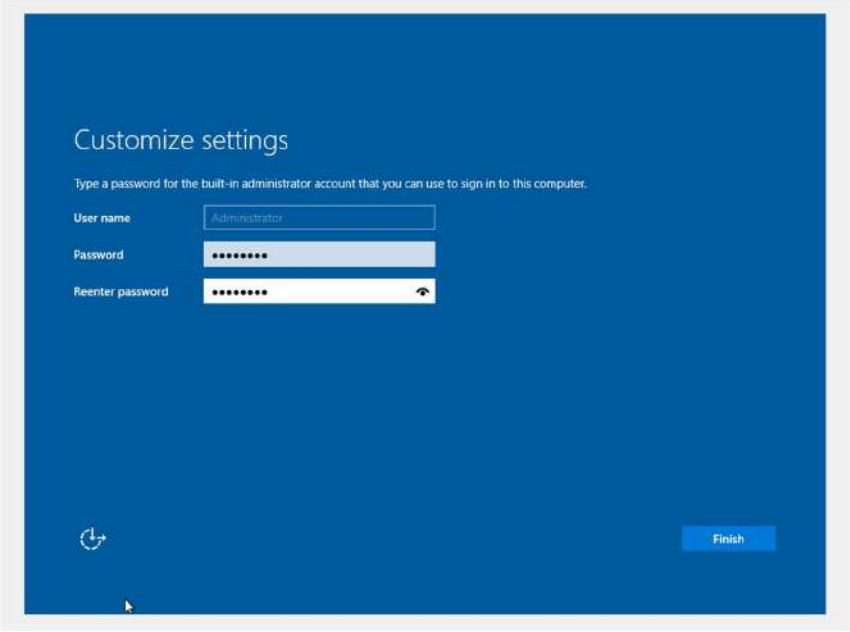


The VM will restart a couple of times during the installation process.

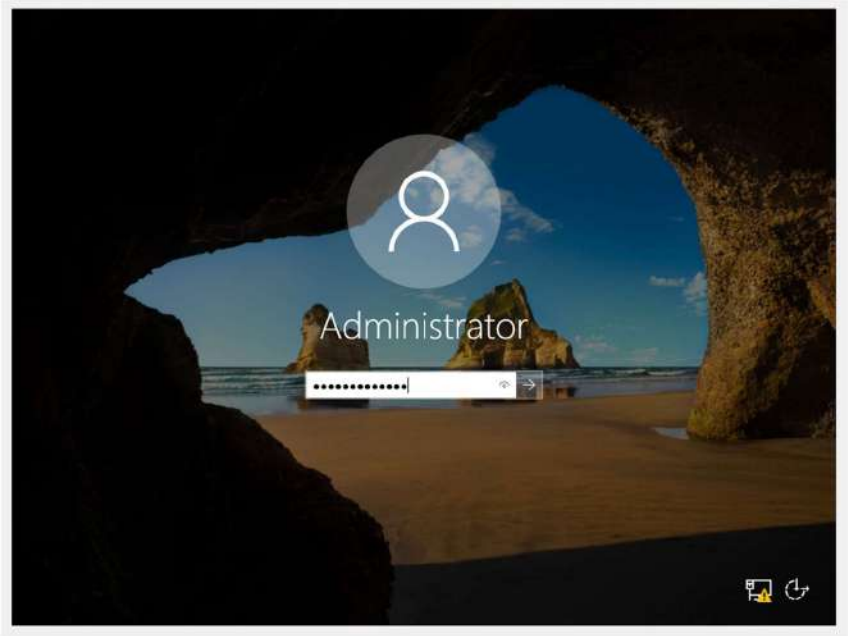


OS Setup & Configuration

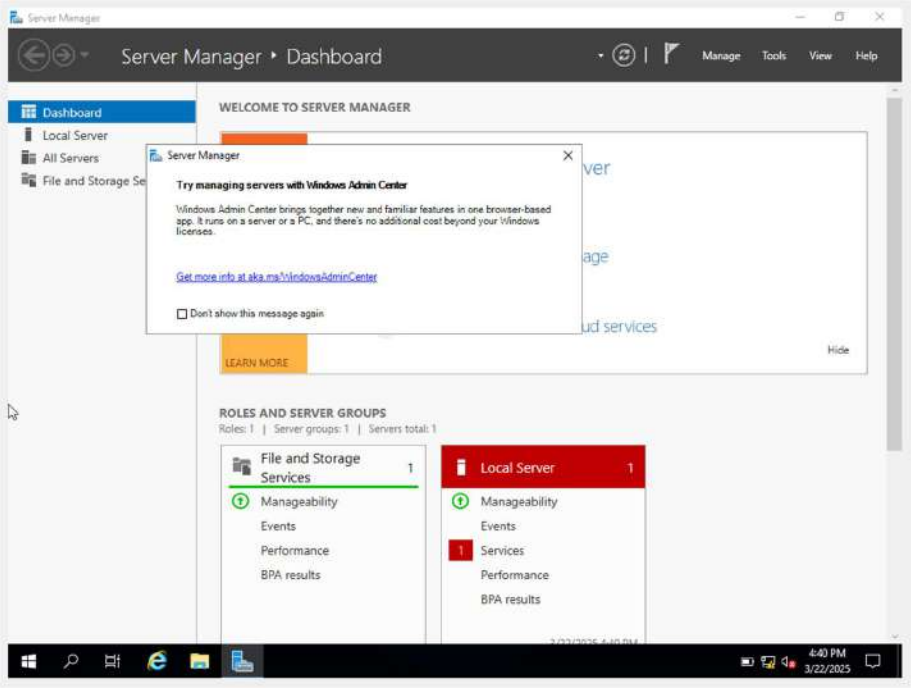
Once the installation is complete we will be asked to set the password for the Administrator account. Once set click on **Finish**.



For login press ctrl + delete button then password is asked

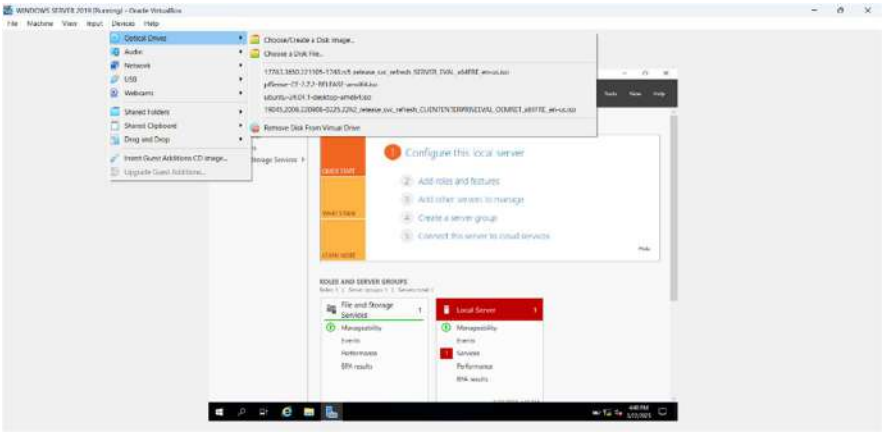


Once we log in. Server Manager will automatically open. A popup will also open asking us to try Windows Admin Center. Click on Don't show this message again and then click on **X** to close the popup.

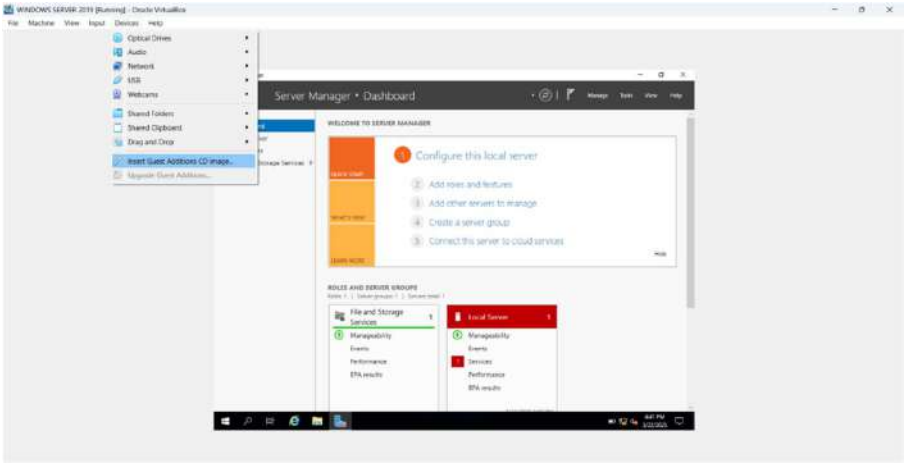


Guest Additions Installation

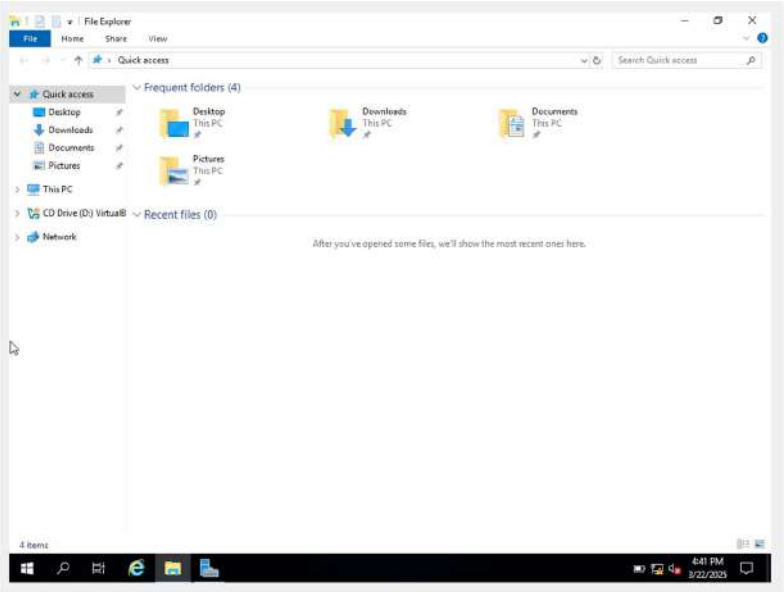
To make the VM screen size bigger we need to install Guest Additions. From the VM toolbar click on **Devices -> Optical Devices -> Remove disk from virtual drive**. This will remove the Windows Server 2019 image from the disk drive.



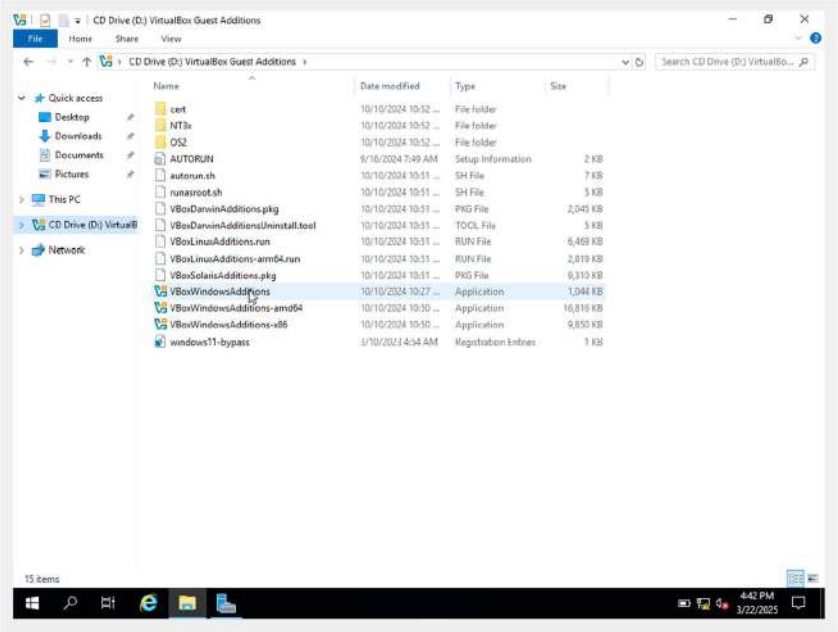
Then select **Devices -> Insert Guest Additions CD image**.



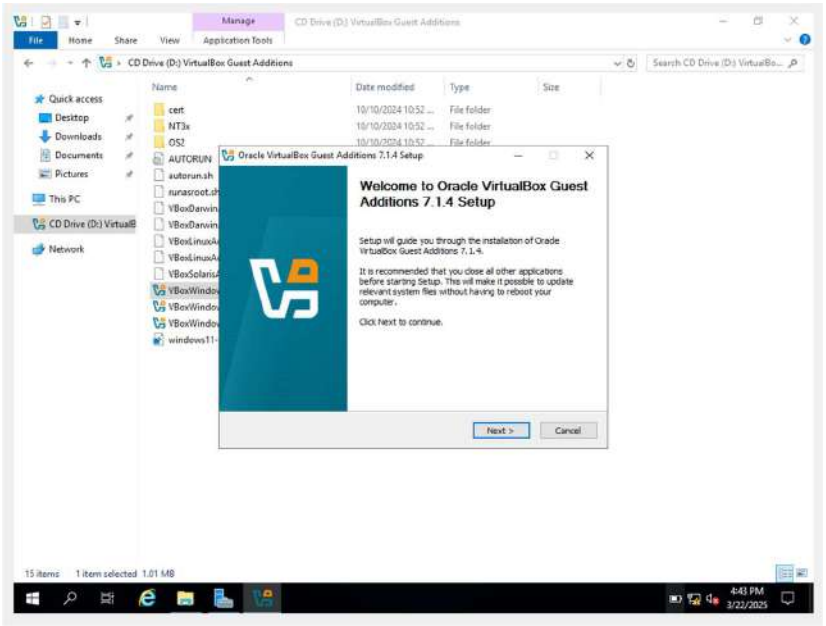
Open file explorer then **CD Drive** option shows click on it



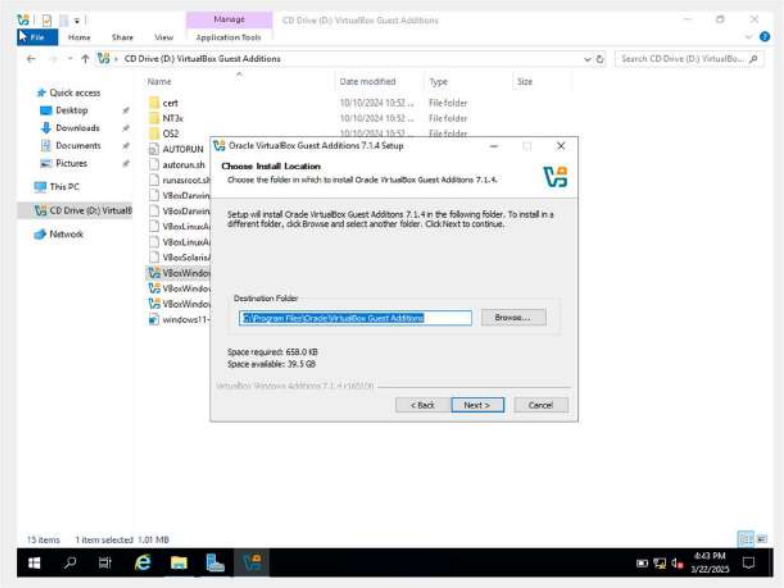
Double-click on **VboxWindowsAdditions** (4th file from bottom) to start the installer.



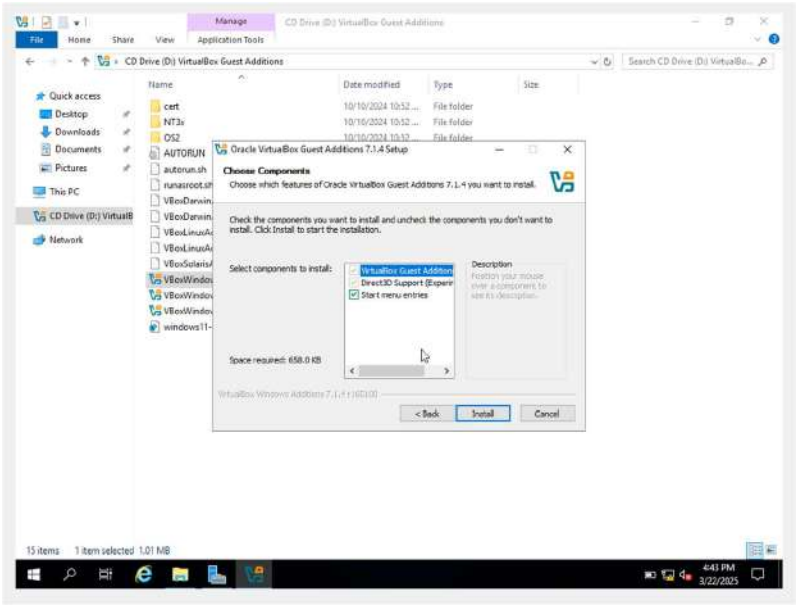
Click on **Next**.



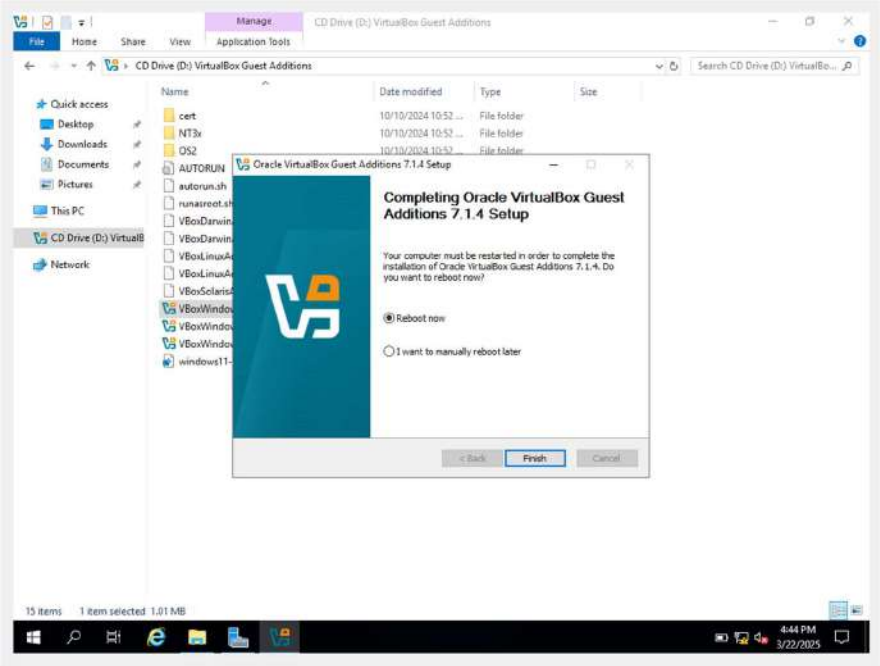
Click on **Next**.



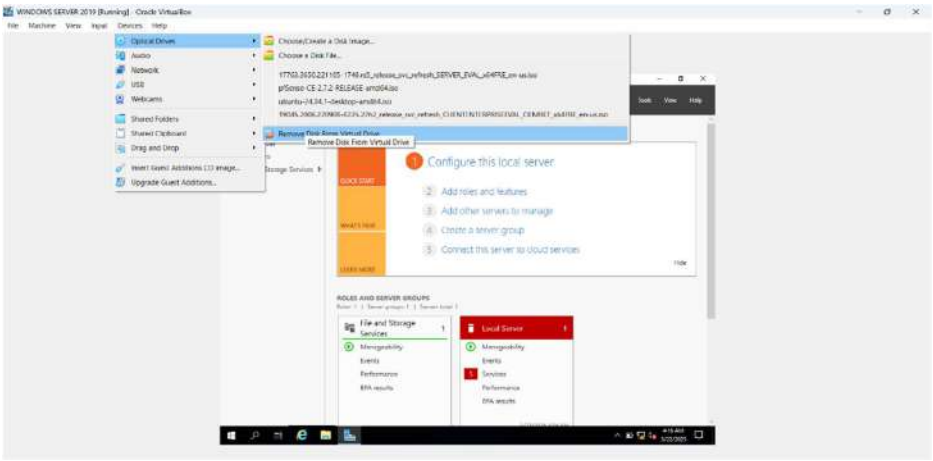
Click on **INSTALL**. For installing the requirement components.



Choose **Reboot now** and click on **Finish**. The VM will restart automatically.



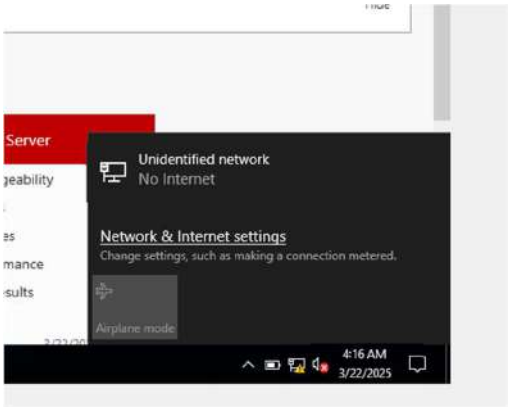
After restart, log into the system. From the VM toolbar click on **Devices -> Optical Drivers -> Remove disk from virtual drive** to remove the Guest Additions image



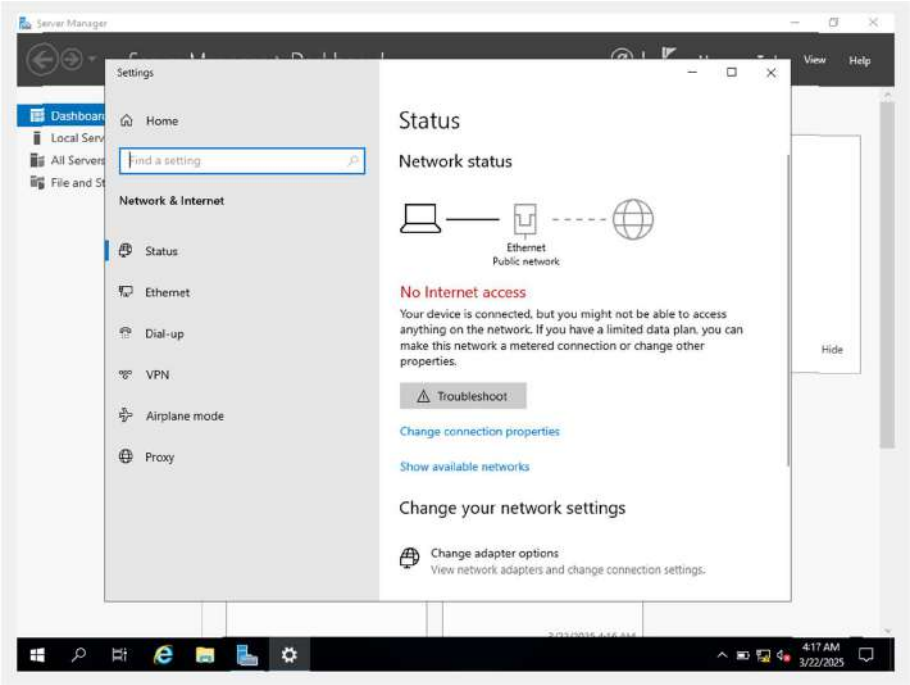
Use the shortcut **Right Ctrl+F** to enter Fullscreen mode. The VM will automatically scale to fill the entire screen. Use the same shortcut to exit Fullscreen mode.

Network Configuration

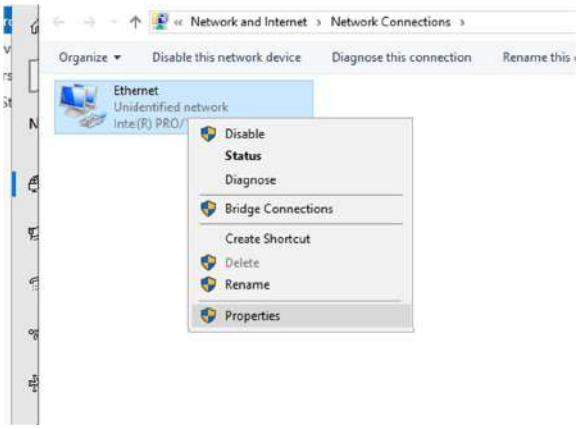
During the pfSense setup module we disabled DHCP on the **AD_LAB** interface because of this our VM will not be automatically assigned an IP address. From the taskbar right-click on the network icon and select **Open Network & Internet settings**.



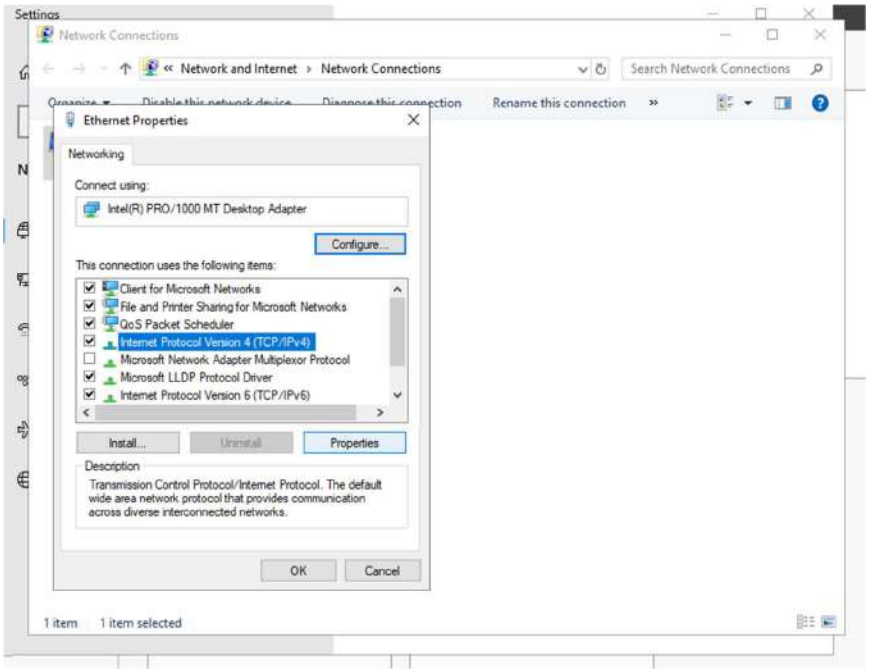
Click on "Change adapter options".



On the Network Connections page, we should see the Ethernet adapter. Right-click on the adapter and select **Properties**.

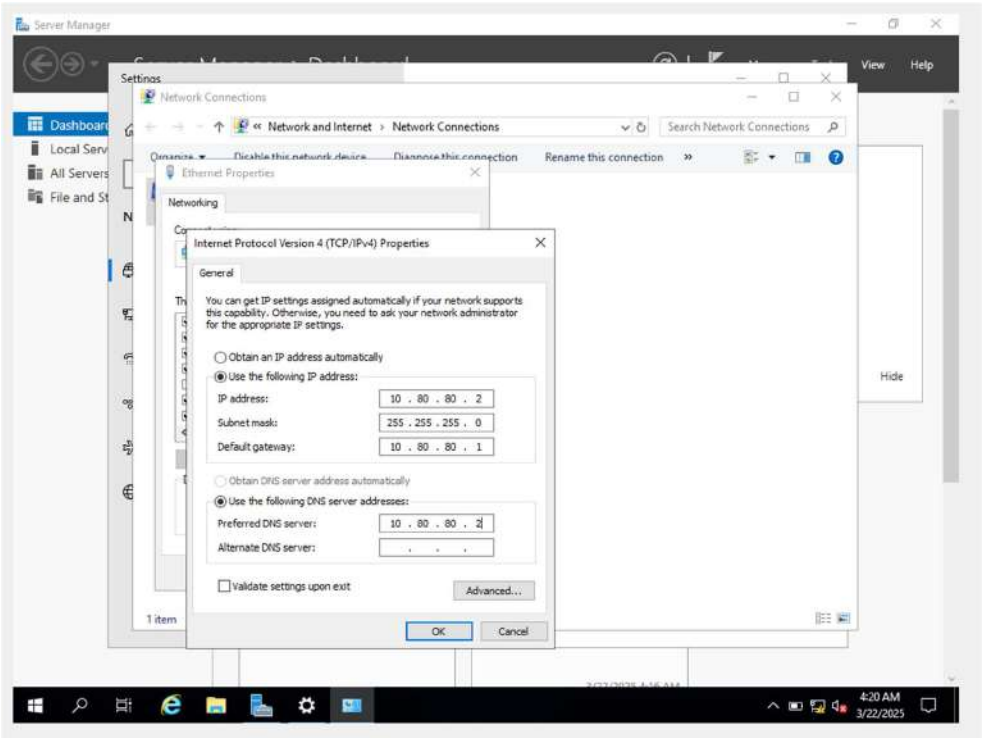


Select **Internet Protocol Version 4 (TCP/Ipv4)** and click on **Properties**.

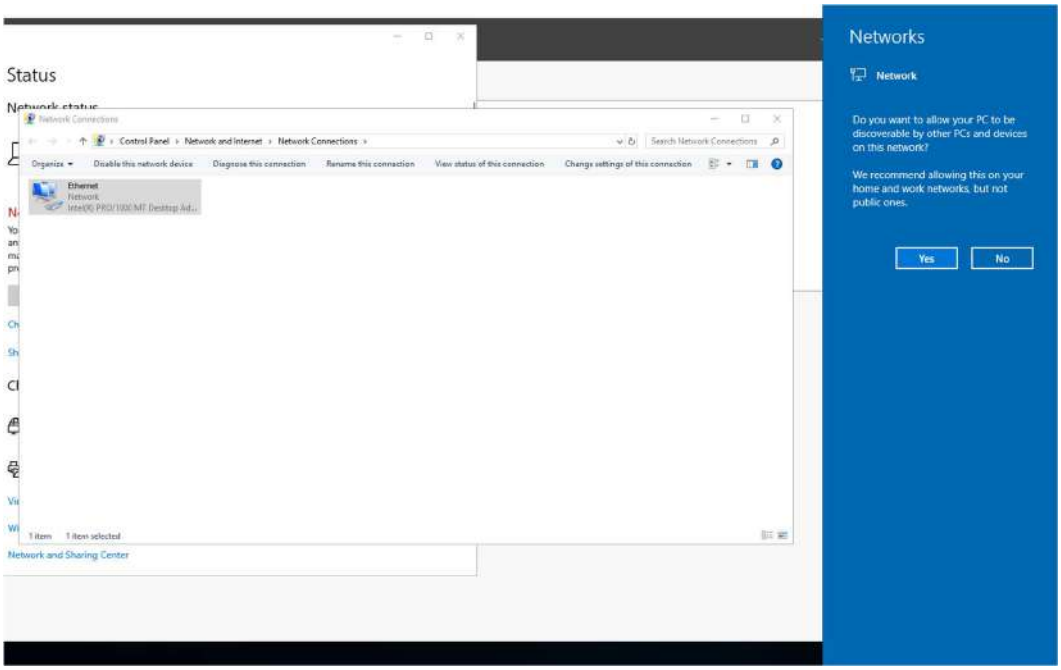


Enter the details as shown below and then click on **OK**. Click on **OK** again to close the Ethernet Properties menu.

IP address: **10.80.80.2**
Subnet mask: **255.255.255.0**
Default gateway: **10.80.80.1**
Preferred DNS Server: **10.80.80.2**

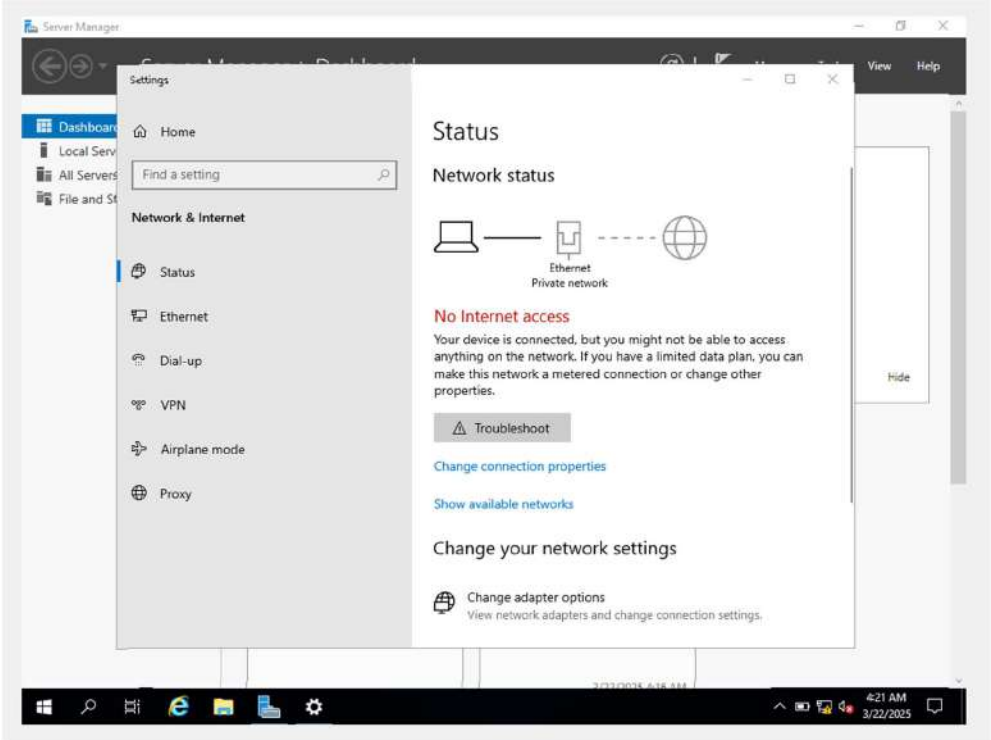


Windows will display a banner to allow internet access click on **Yes**.



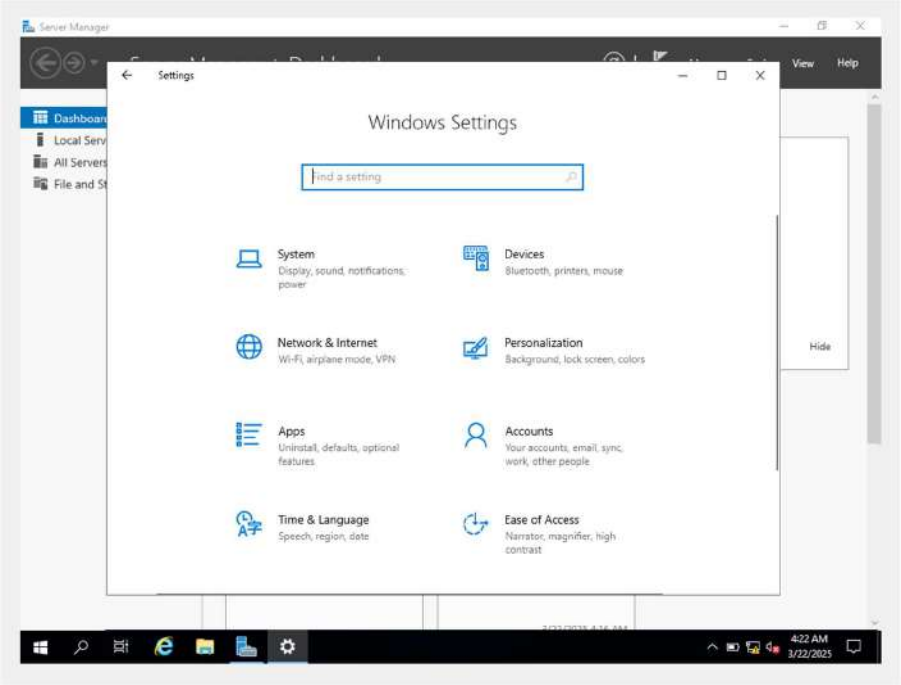
Close the Network Connections page.

In the Settings app click on the **Home** button (above search bar).

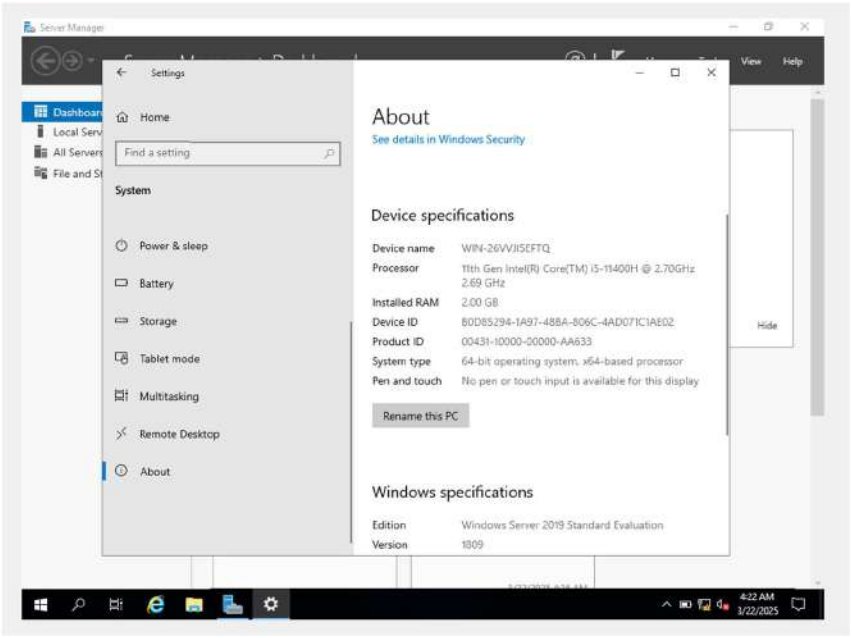


Renaming the System

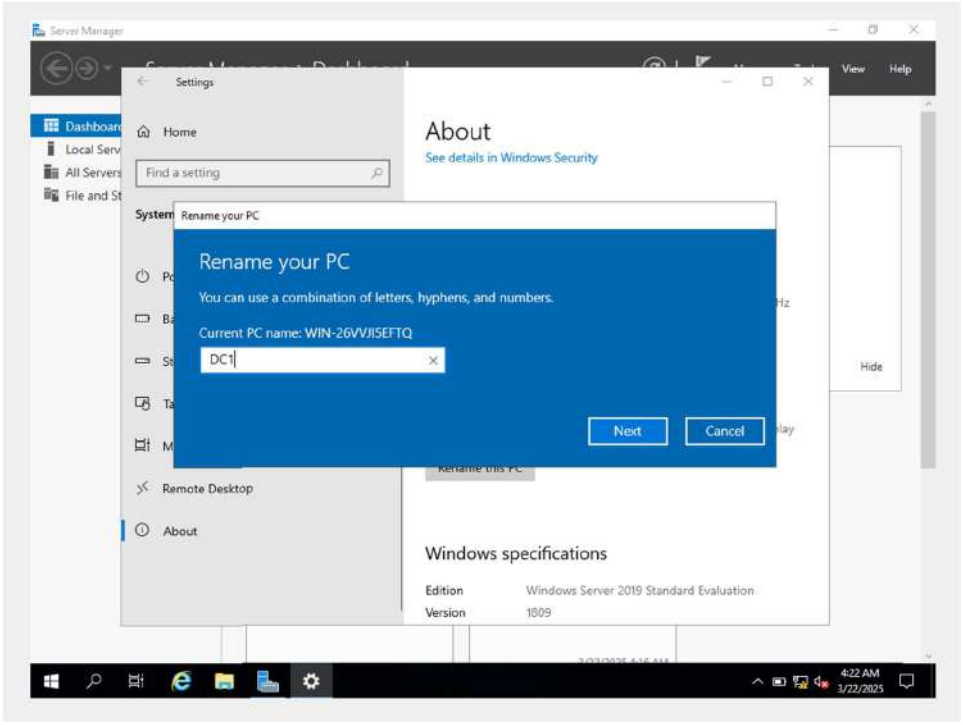
Before we can set up the machine to be a Domain Controller let us rename the PC. Select "System".



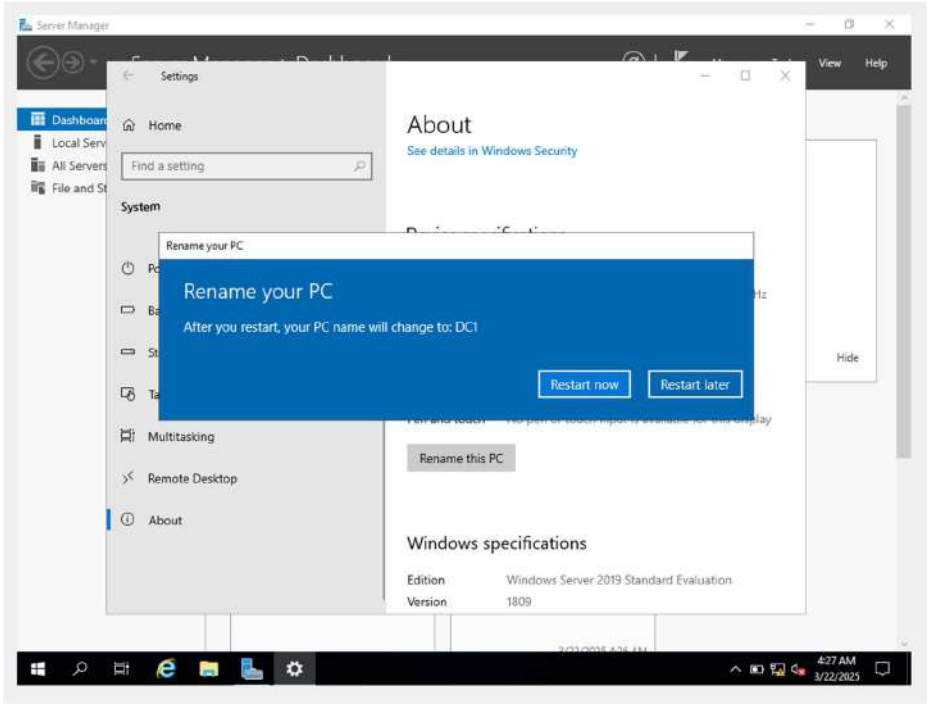
Click on About on the sidebar and then click on the "Rename this PC" button.



Give the PC an easy-to-remember name and then click on **Next**.

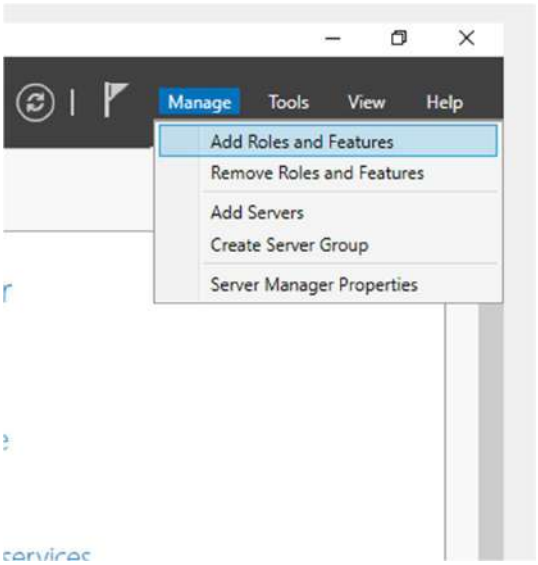


Click on "Restart now" for the changes to take effect.

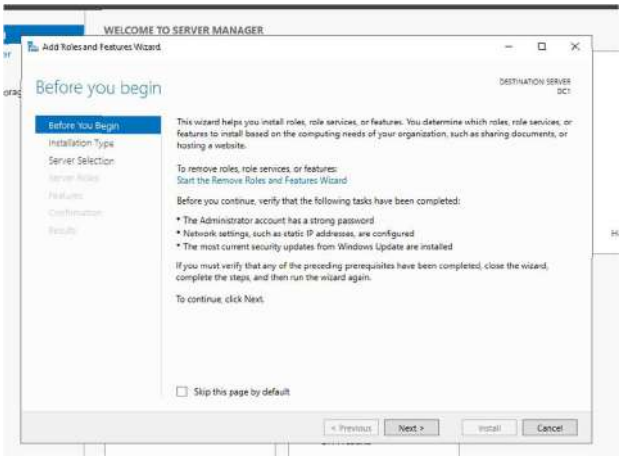


Active Directory & DNS Installation

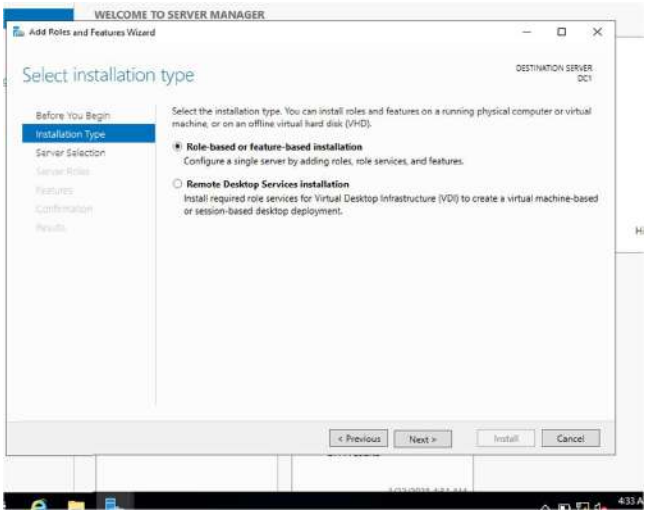
After login wait for Server Manager to load. Click on the **Manage** button from the top right corner and select "Add Roles and Features".



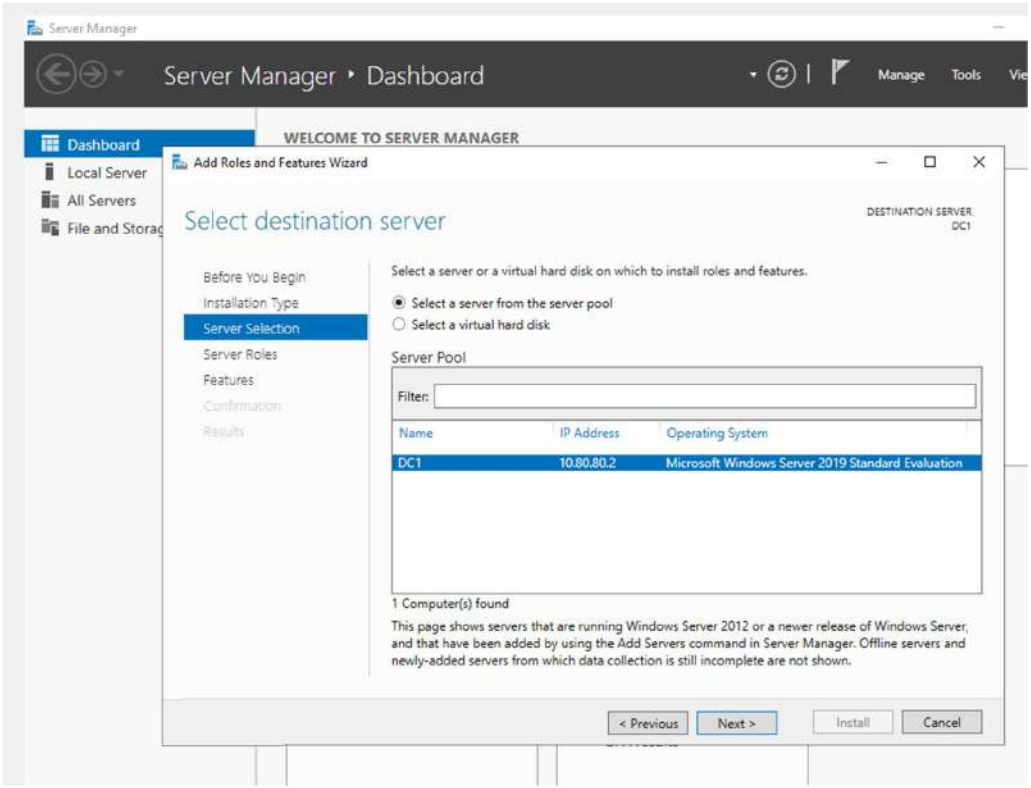
Click on **Next**



Click on **Next**

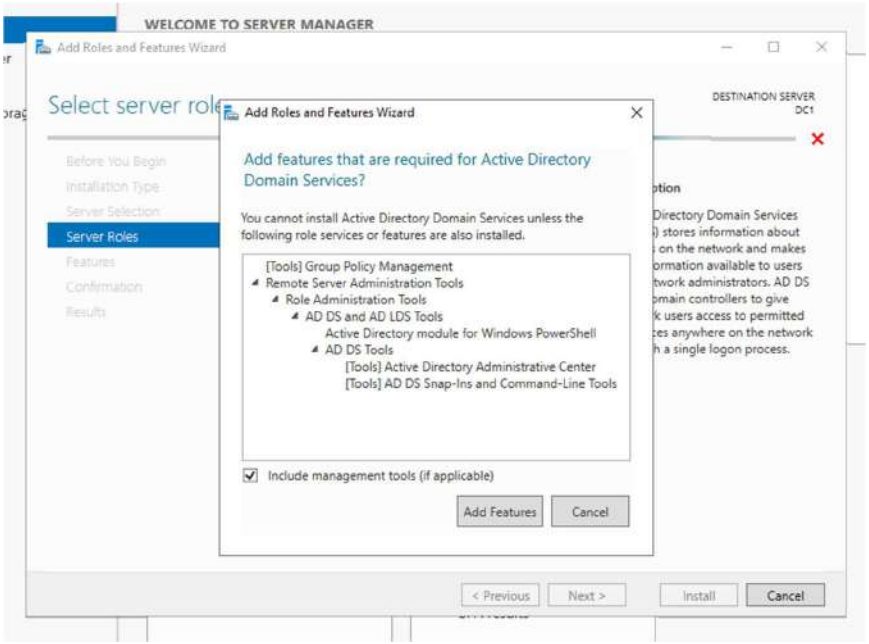


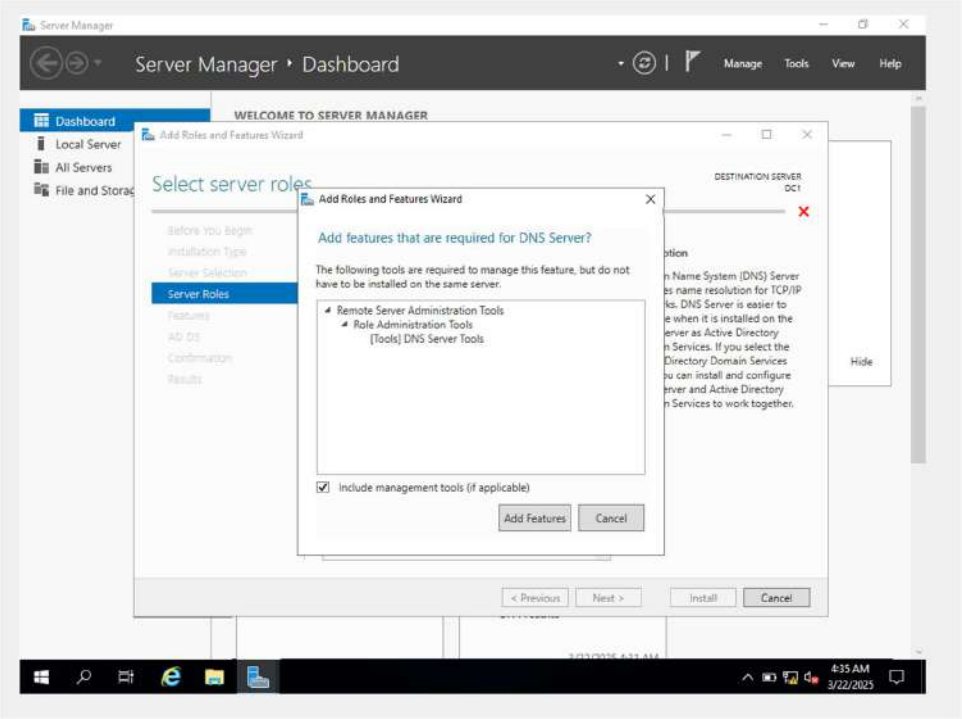
Click on **Next**



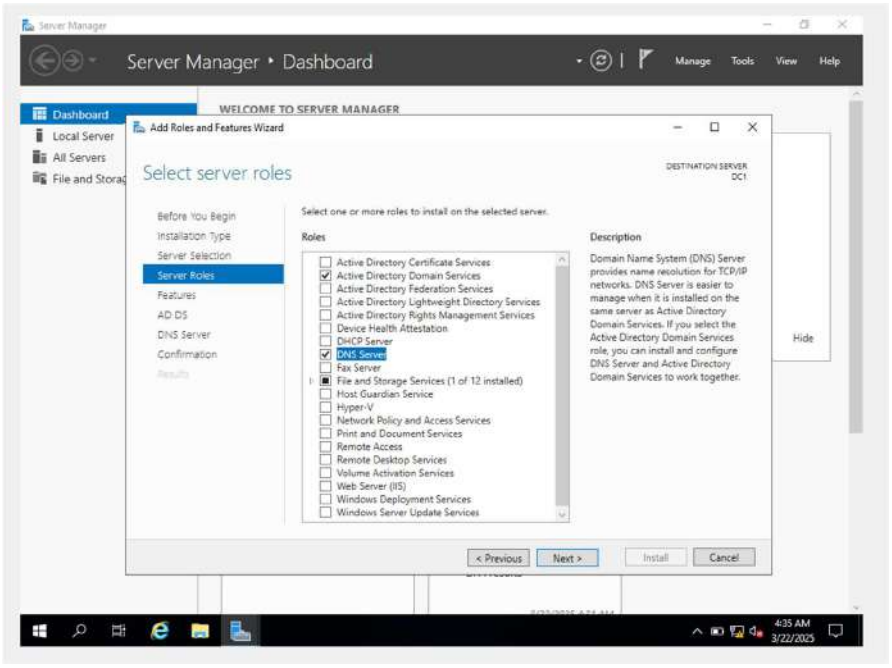
On this page enable "Active Directory Domain Services" and "DNS Server".

When you enable a feature the "Add Roles and Features Wizard" will open click on "Add Features" to confirm the selection.

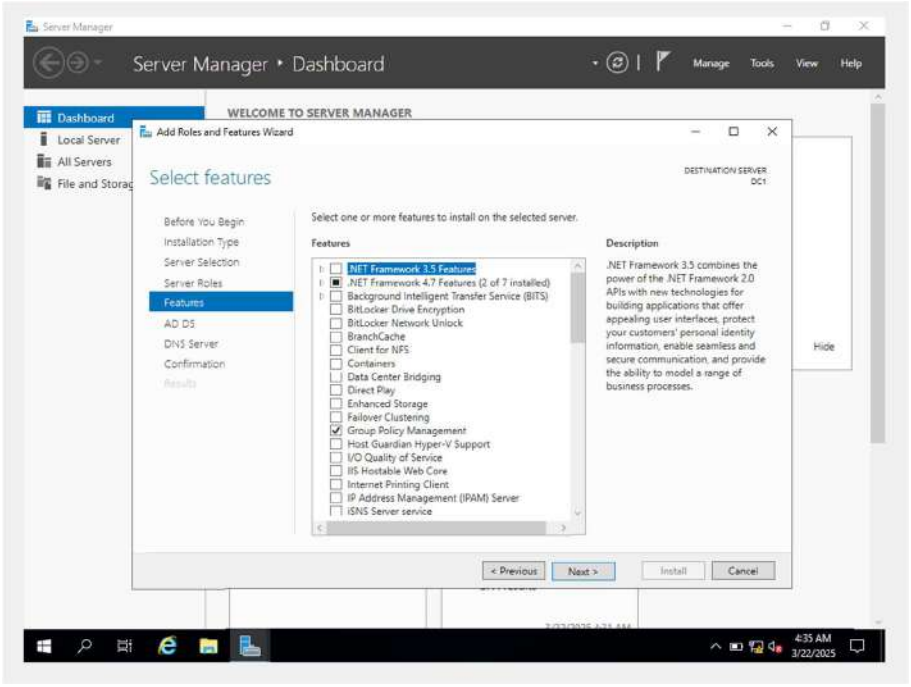




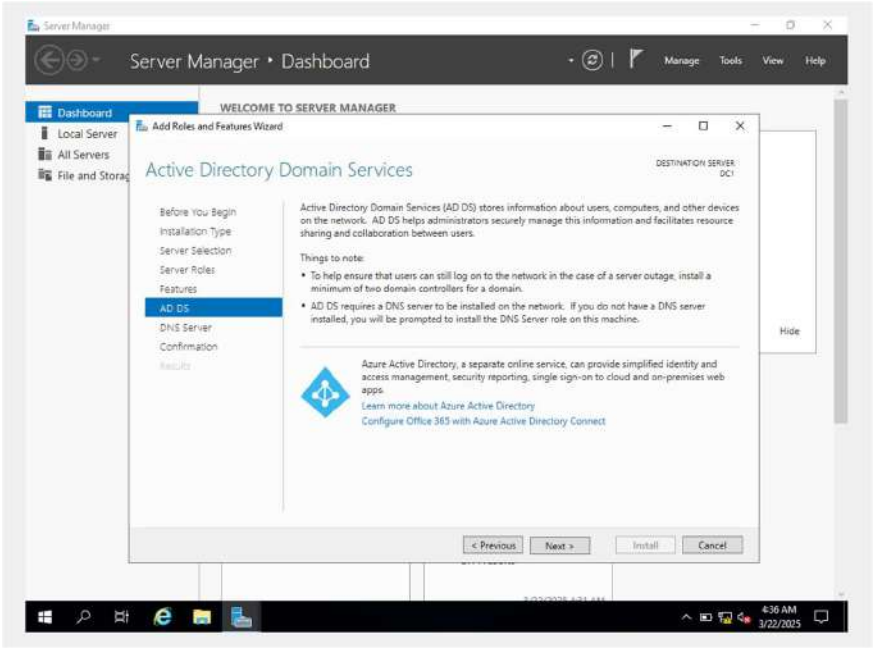
Once both the features are selected click on **Next** to proceed with installation.



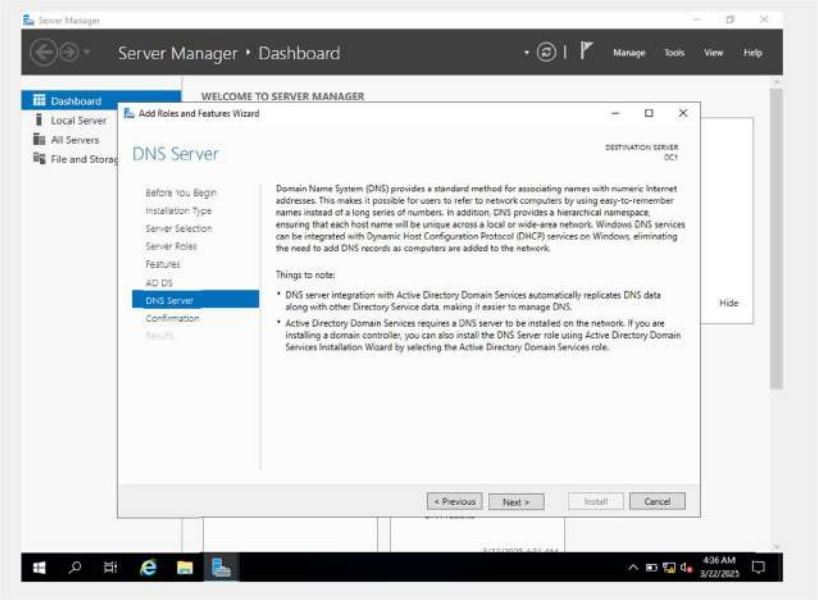
Click on **Next**



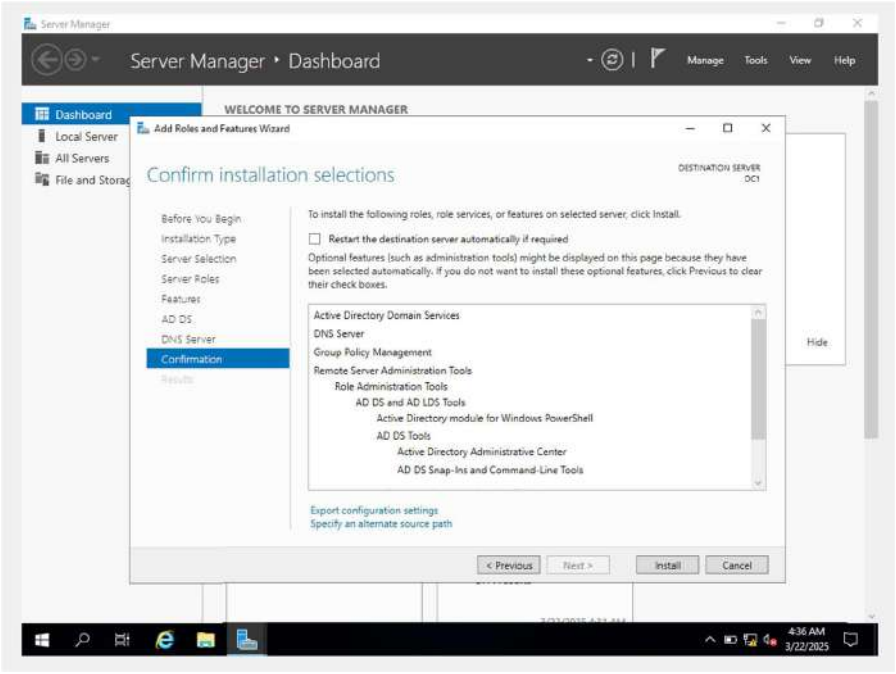
Click on **Next**



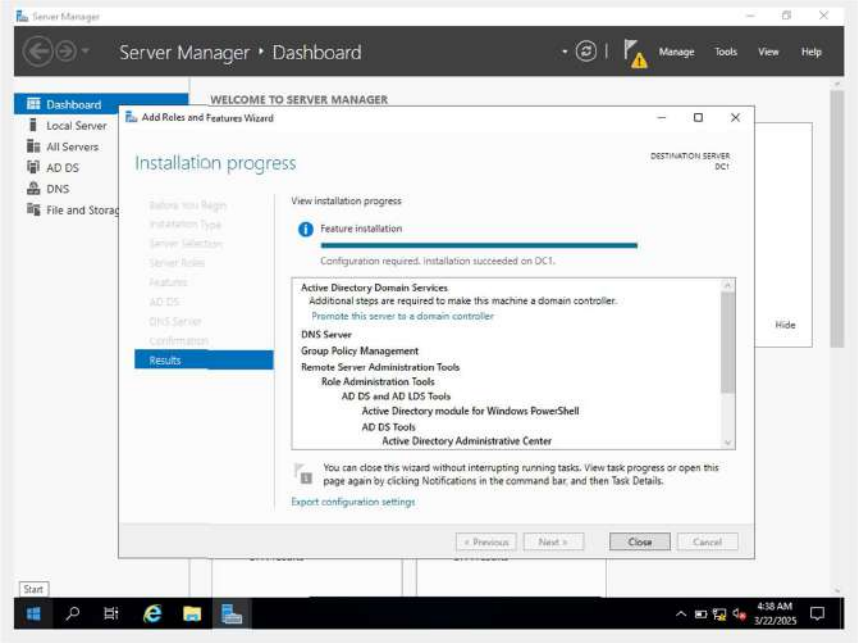
Click on **Next**



Here click on **Install** to start the installation of the selected features.

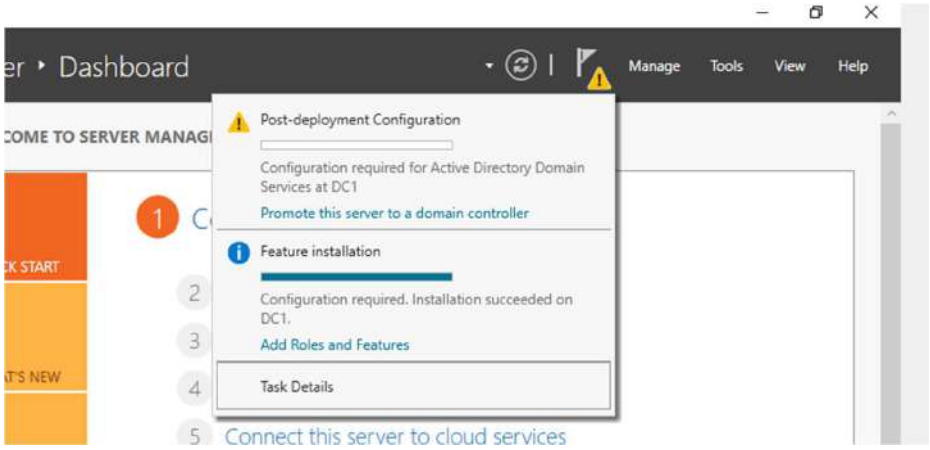


Once the installation is complete click on **Close** to exit the Wizard.

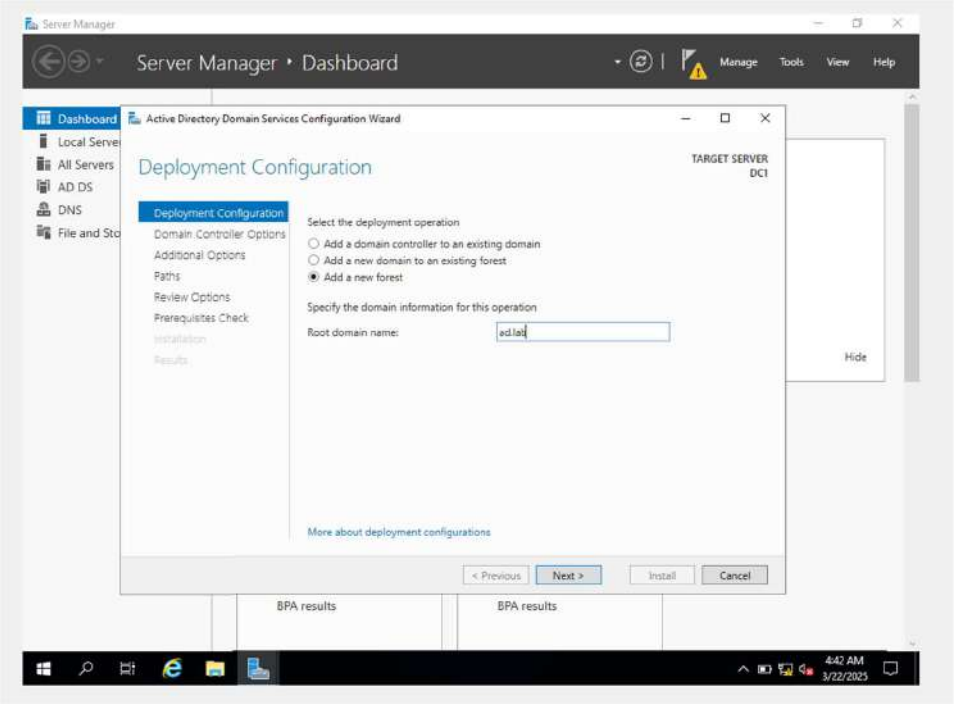


Active Directory Configuration

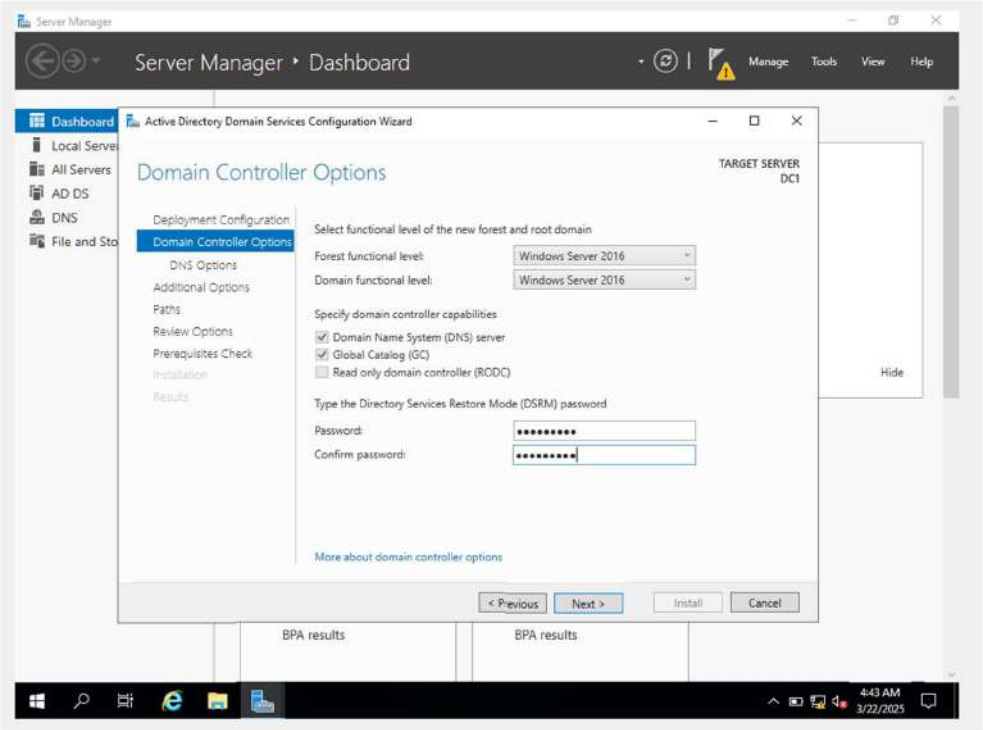
Click on the Flag icon present in the top right of the toolbar in Server Manager. From the dropdown click on "Promote this server to a domain controller".



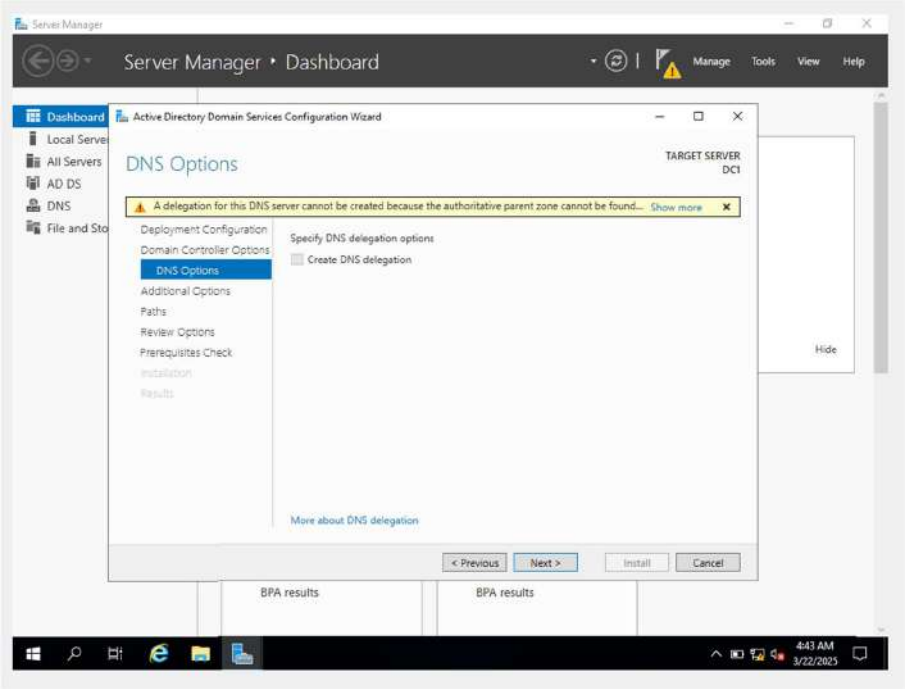
The AD Domain Servers Configuration Wizard will open. For deployment operation select **Add a new Forest**. Give the domain a name. For my setup, I will be using the domain name **ad.lab**. After selecting the name click on **Next**.



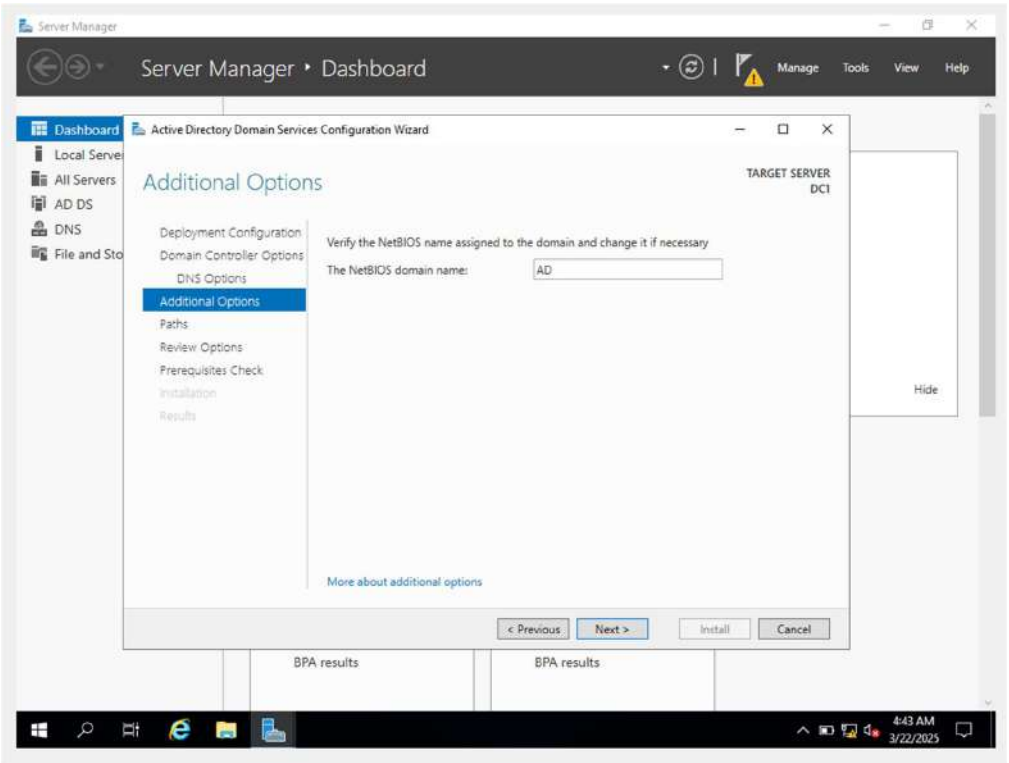
On this page enter a password to use for using the AD Restore feature.



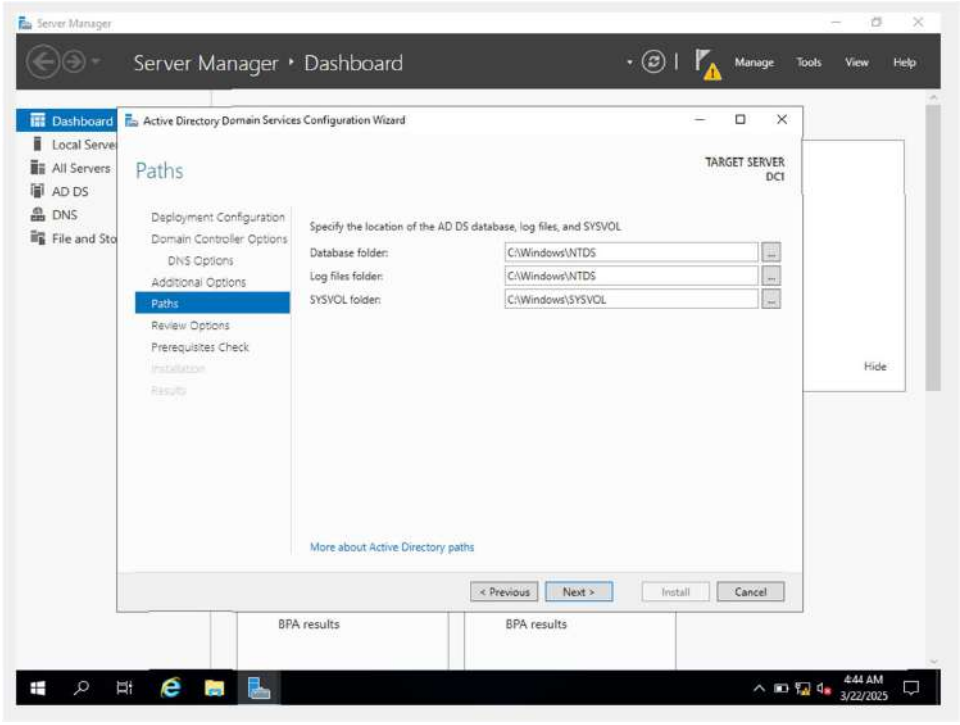
Ignore the warning that is shown and click on **Next**.



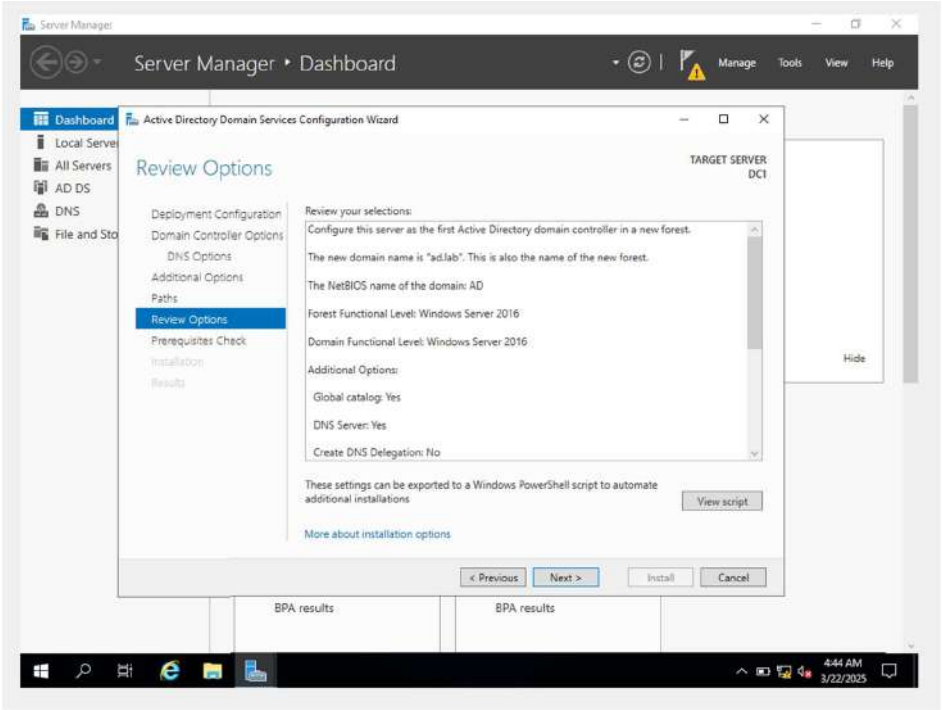
The NetBIOS name should automatically be filled. It will be the first part of the domain name. Click on **Next** to continue.



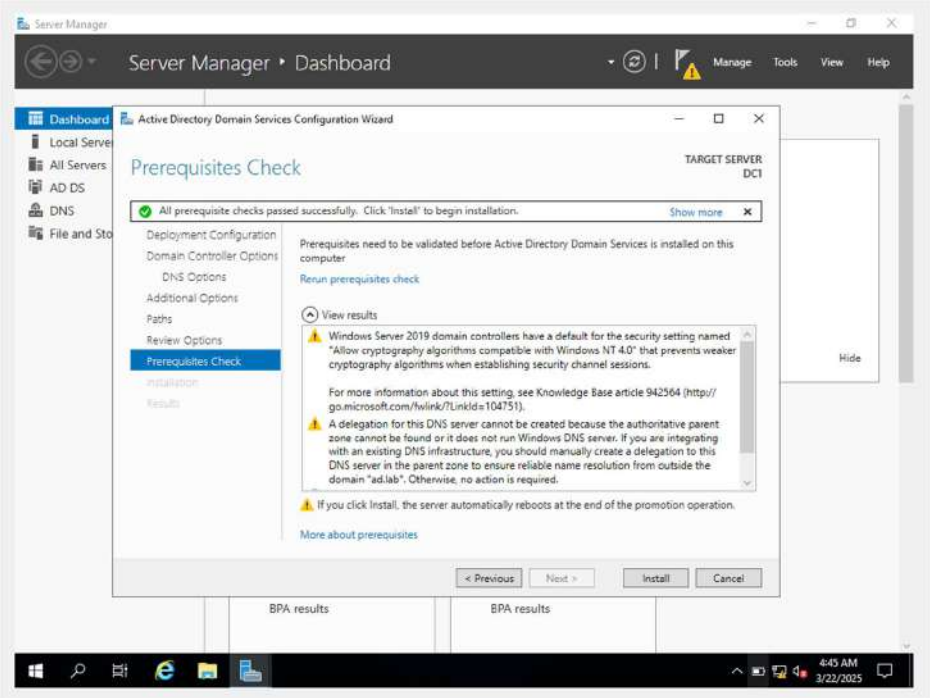
Click on **Next**.



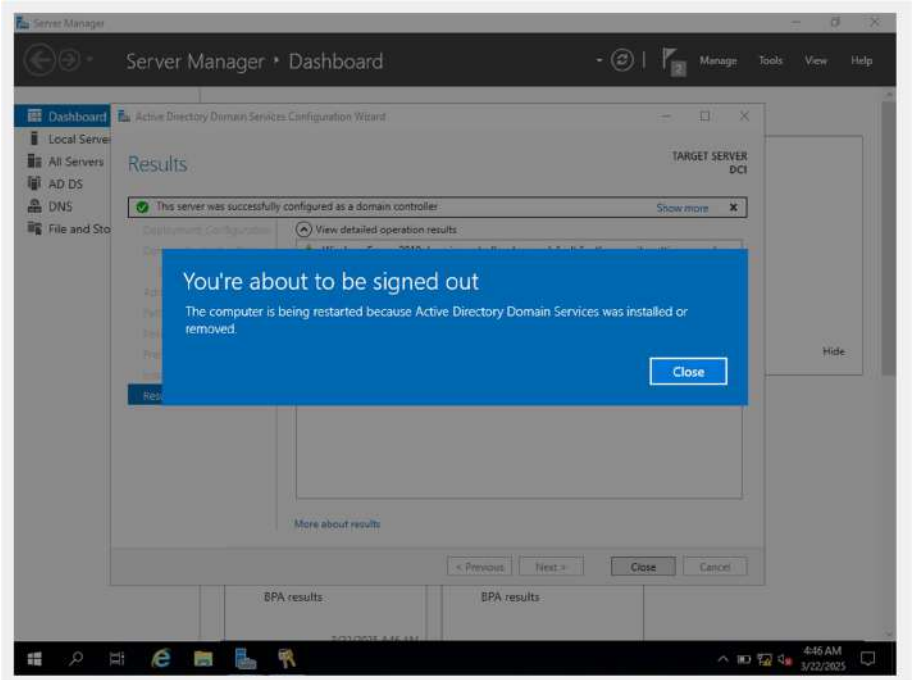
Click on **Next**.



Click on **Install** to start the Domain Services setup process.



Once the install process is complete the machine will need to restart. Click on **Close** to reboot the system.

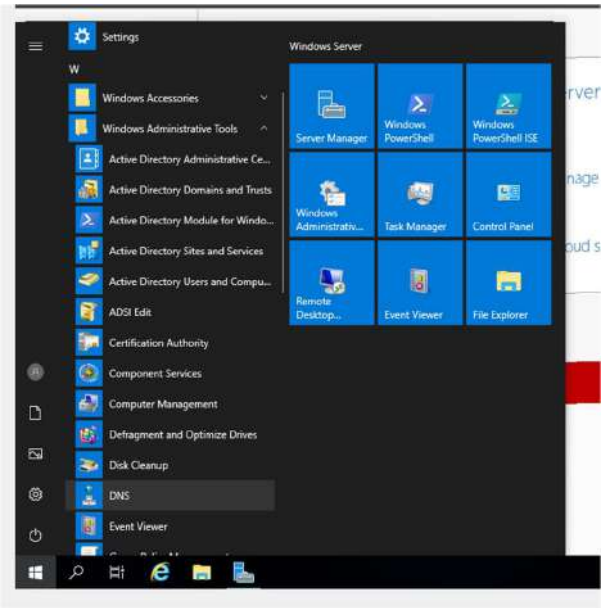


On restart, you will notice that the name that is shown on the login page has changed. The first part of the domain name is prepended to the username. This means the machine has successfully been configured as the domain controller. Log in using the Administrator password.

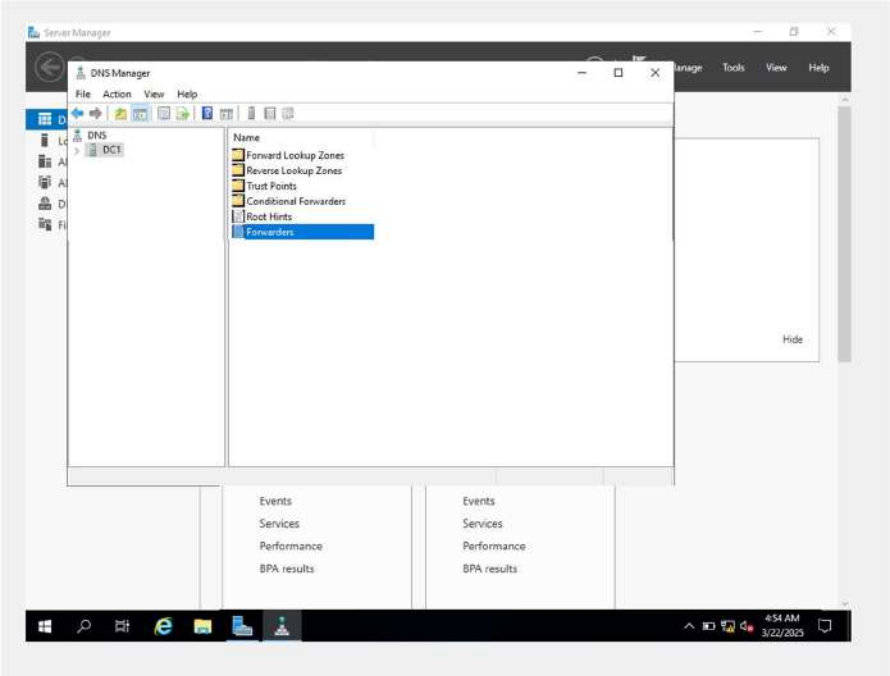
DNS Configuration

Since we enabled DNS on this machine (Domain Controller). This machine (DC) will act as the DNS server for devices that are connected to the **ad.lab** environment. For the DNS service to function properly we need to configure a Forwarder. Forwarder is the device to which the DNS queries will be sent when the DC cannot resolve it. In our case, we need to forward the request to pfSense. The DNS service of pfSense will then perform the lookup.

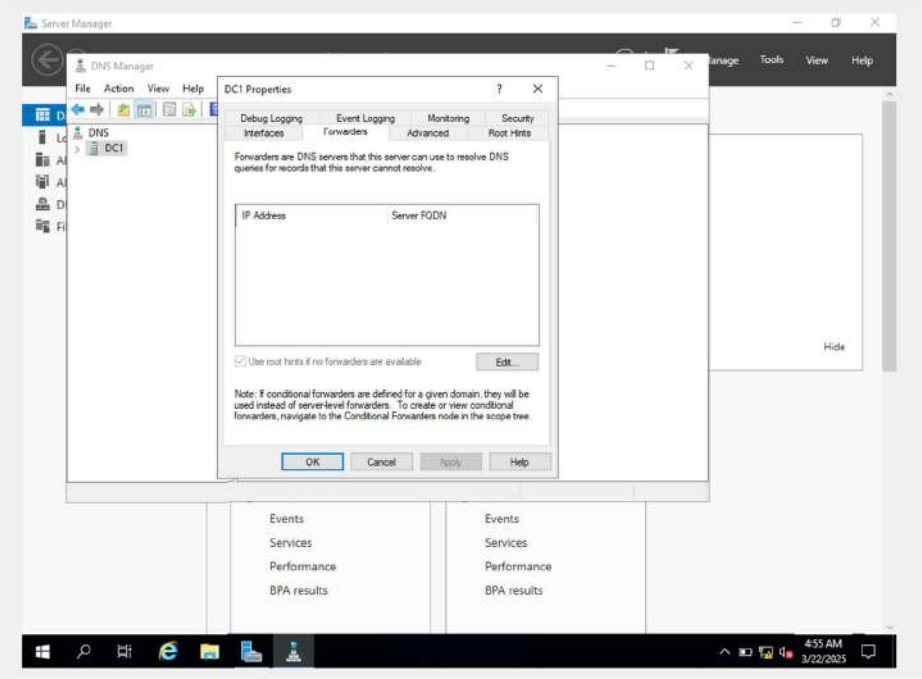
Open the Start menu expand the "Windows Administrative Tools" folder and select **DNS**.



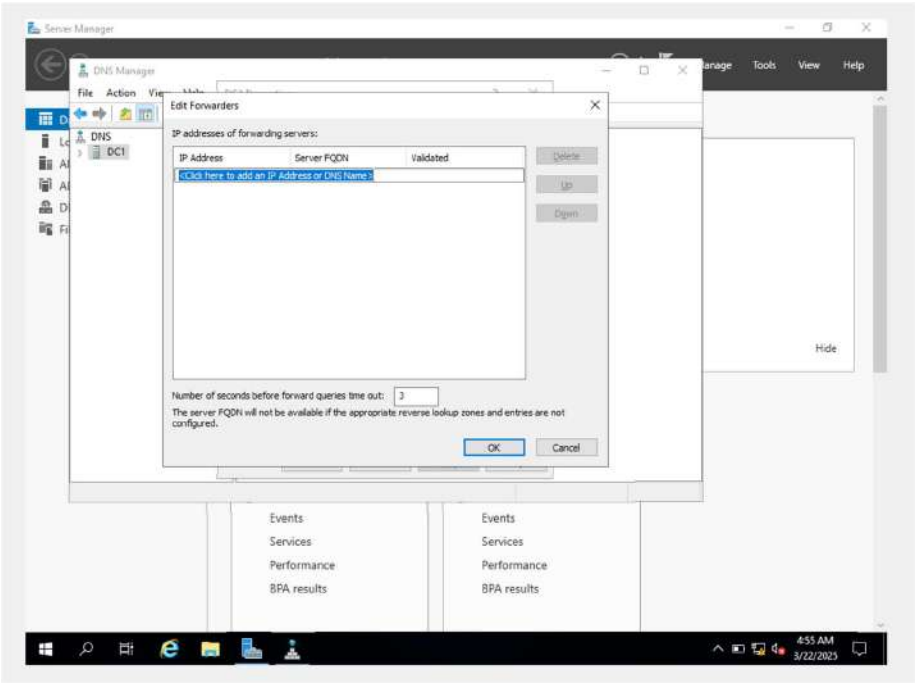
In the sidebar select the Domain Controller (in my case DC1) and from the right menu double-click on "Forwarders".



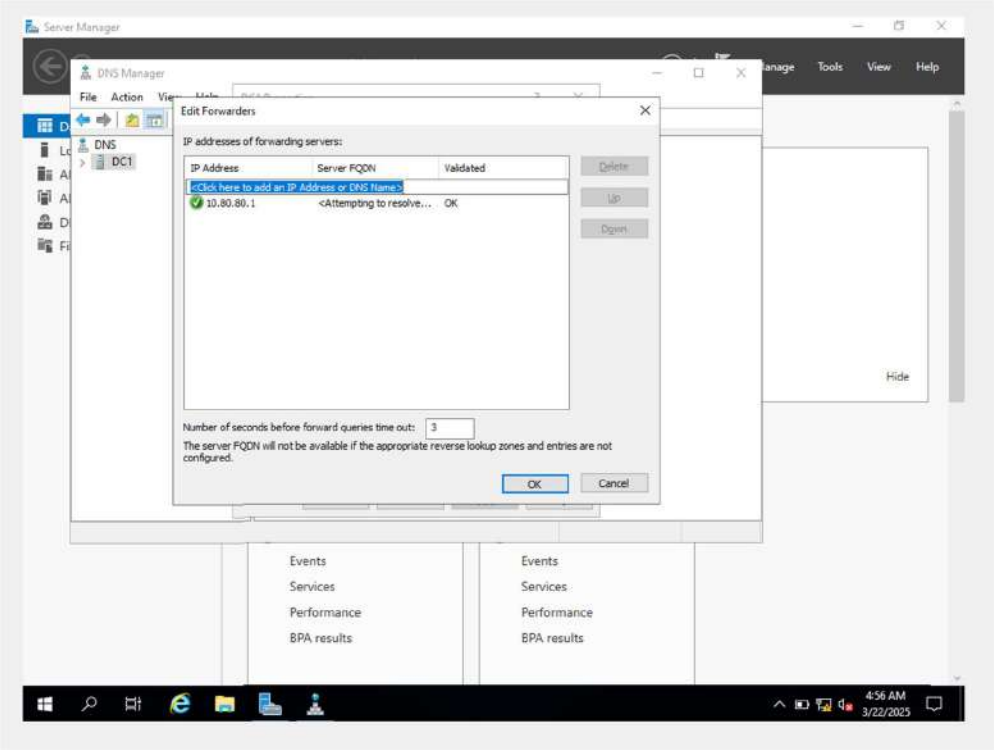
Go to **Forwarders -> Edit**.



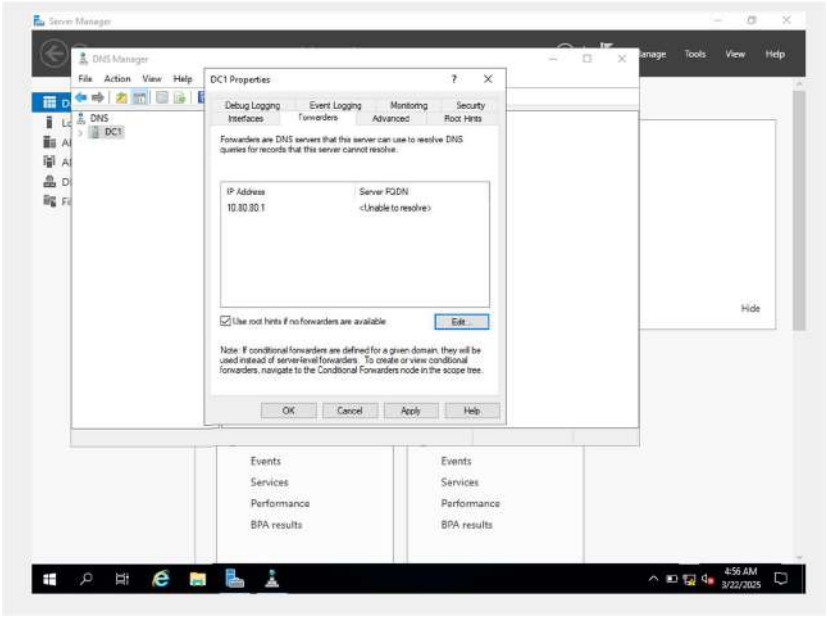
This will open the Forwarder configuration page. Enter the IP address of the **AD_LAB** interface (**10.80.80.1**) and press **Enter**.



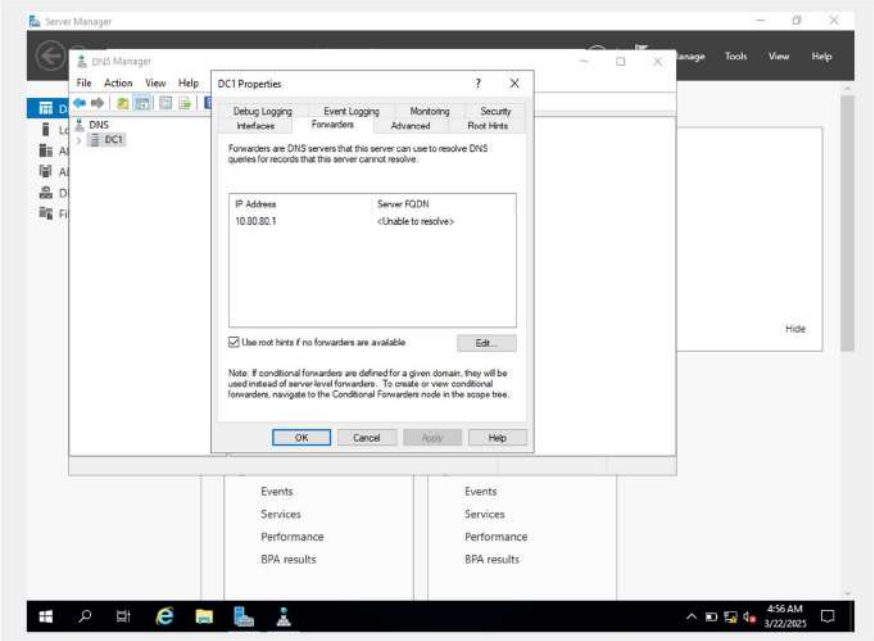
Once added. Click on **OK** to confirm the change.



Click on **Apply** .



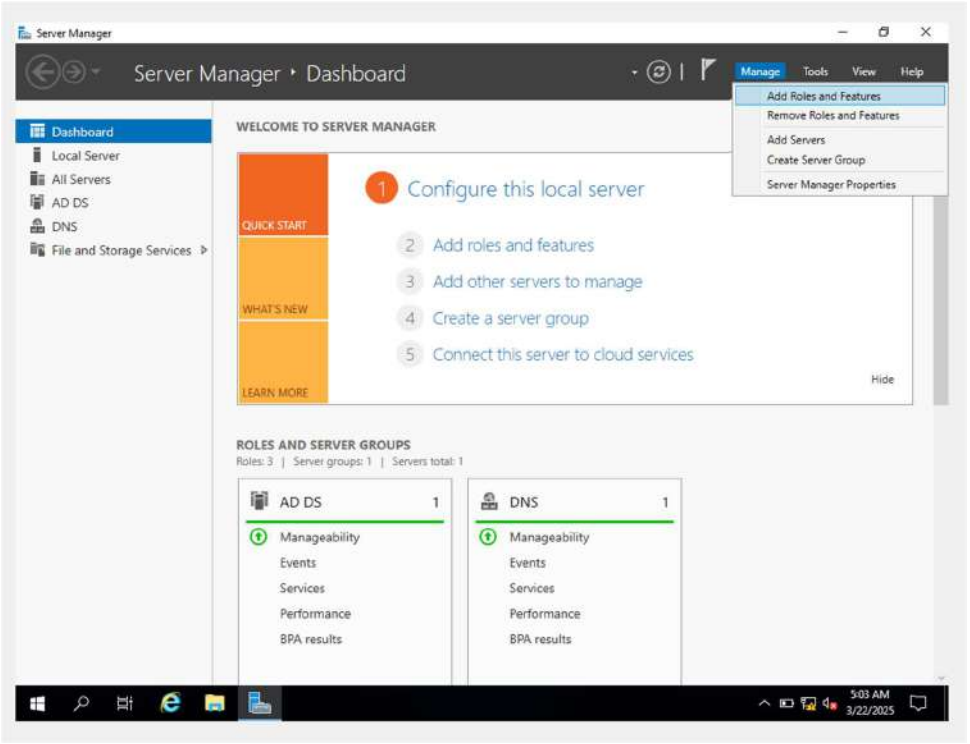
then **OK** to save the changes.



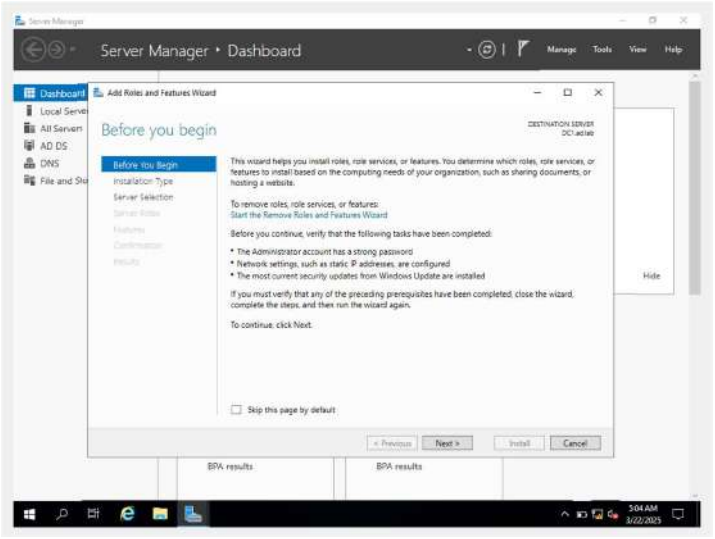
DHCP Installation

Since DHCP is disabled on the **AD_LAB** interface when new devices are added they will not be assigned an IP address. We will enable the DHCP service on the DC. Once set devices that connect to the **AD_LAB** network will be automatically assigned an IP address by the Domain Controller DHCP server.

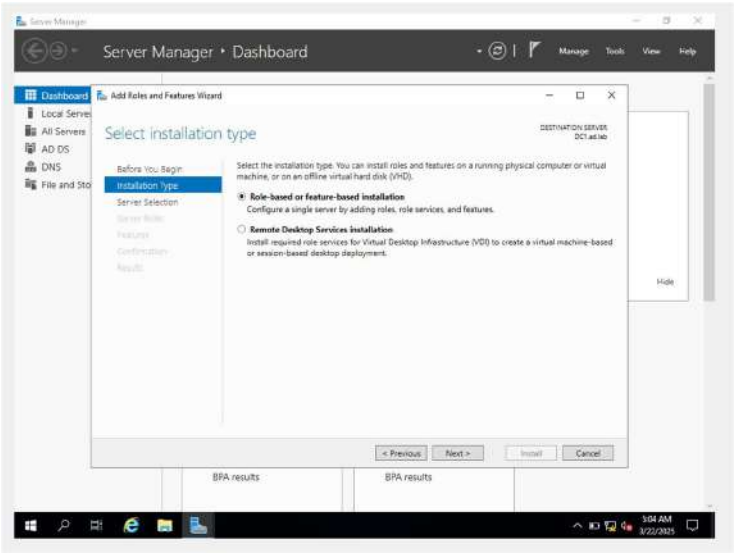
Click on Manage from the toolbar in Server Manager. Then choose "Add Roles and Features".



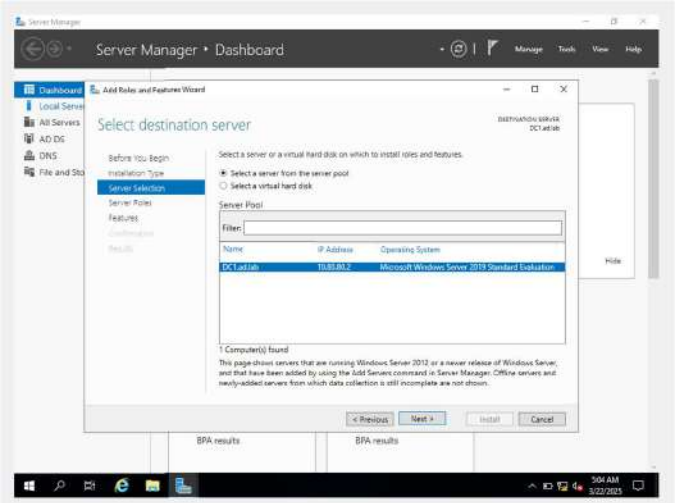
Click on **Next**.



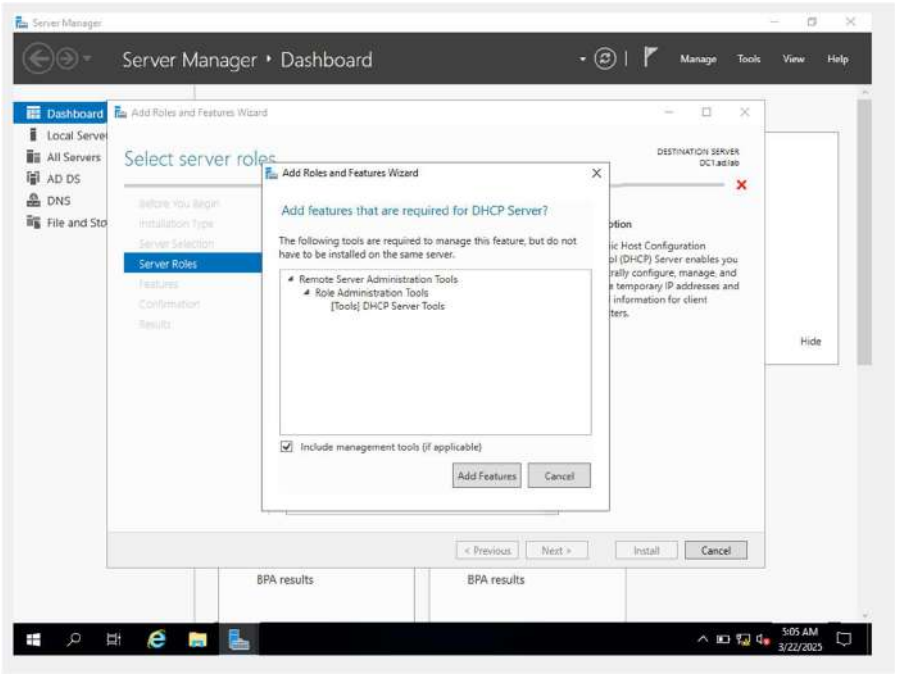
Click on **Next**.

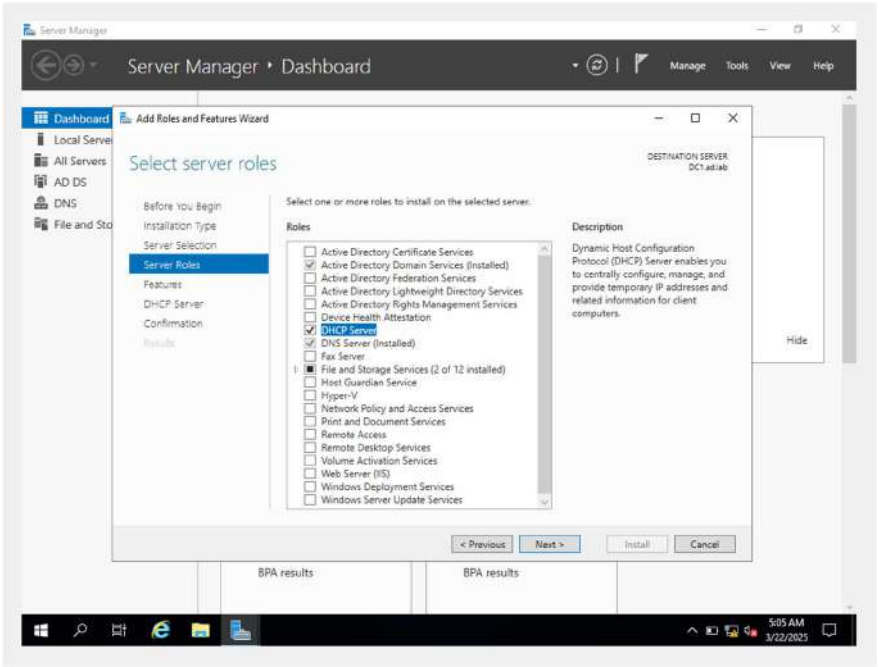


Click on **Next**.

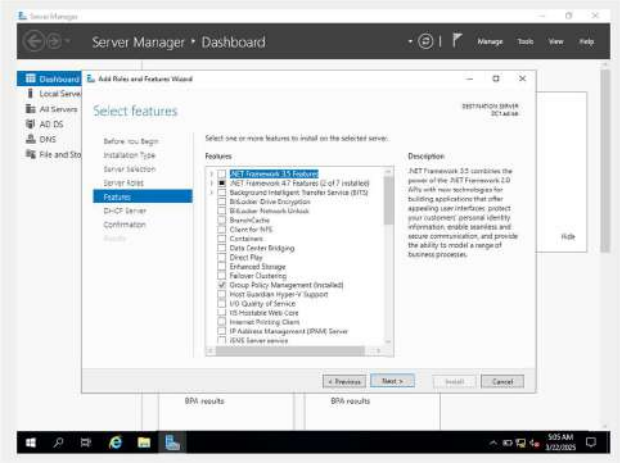


Enable “DHCP Server” then click on “Add Features”.

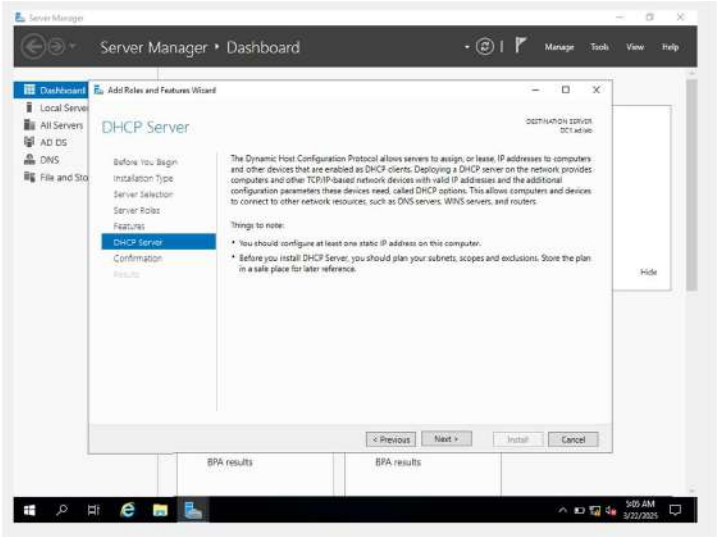




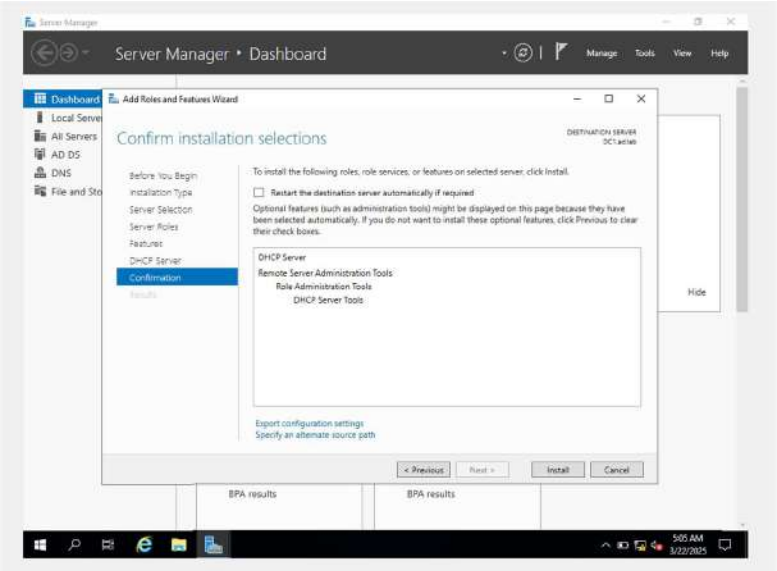
Click on **Next**.



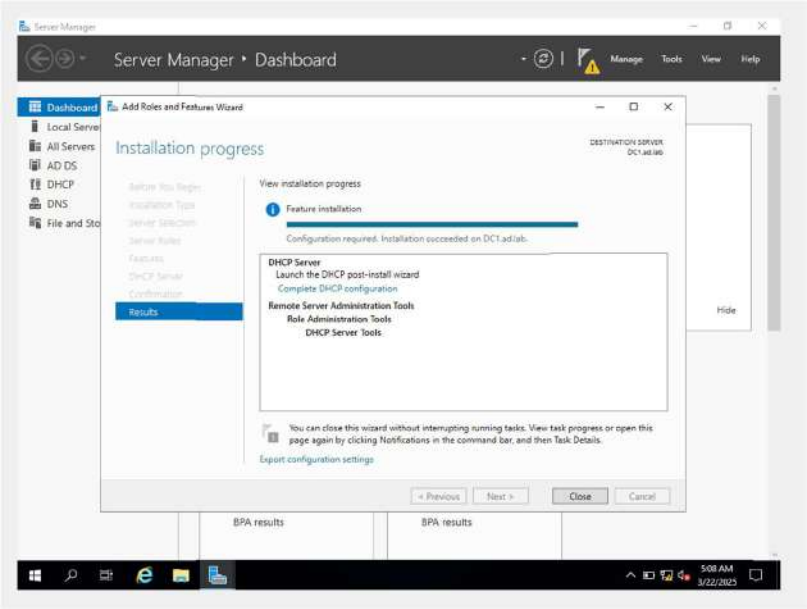
Click on **Next**.



Click **Install** to enable DHCP.

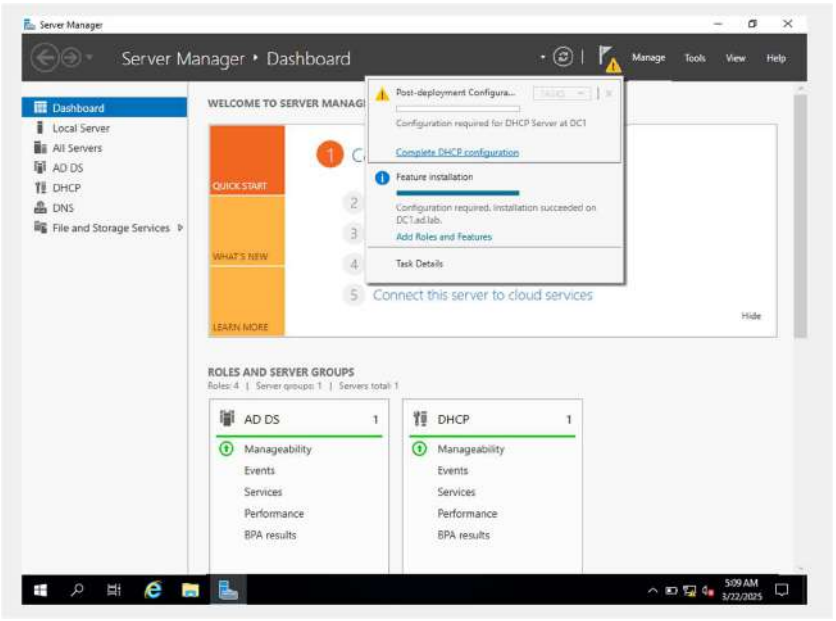


After completion Close it.

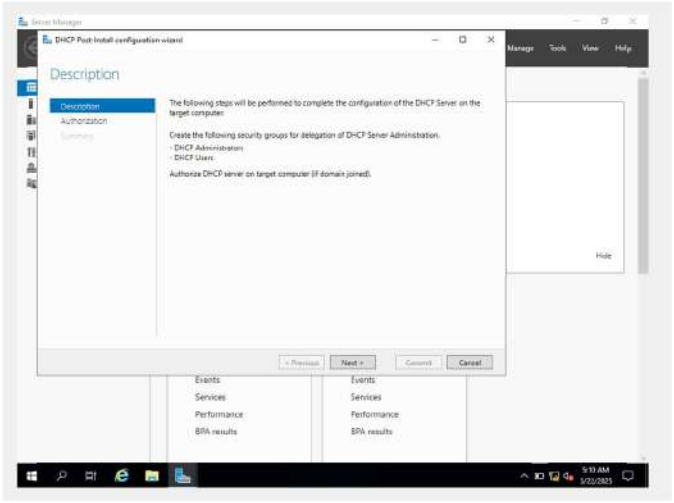


DHCP Configuration

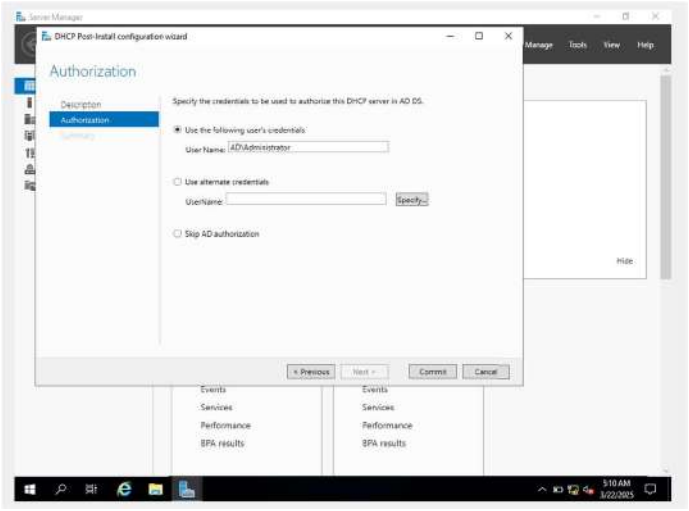
After the installation is complete click on the Flag present in the toolbar of Server Manager and click on "Complete DHCP configuration".



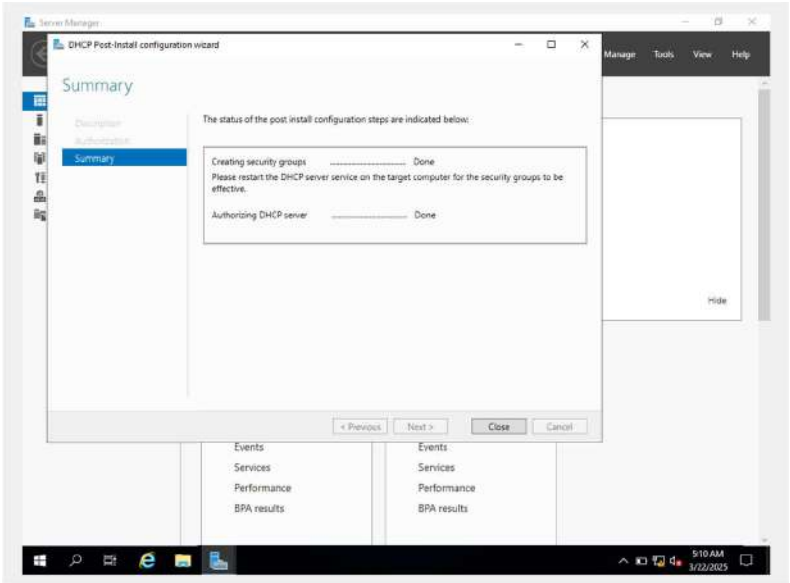
Click on **Next**.



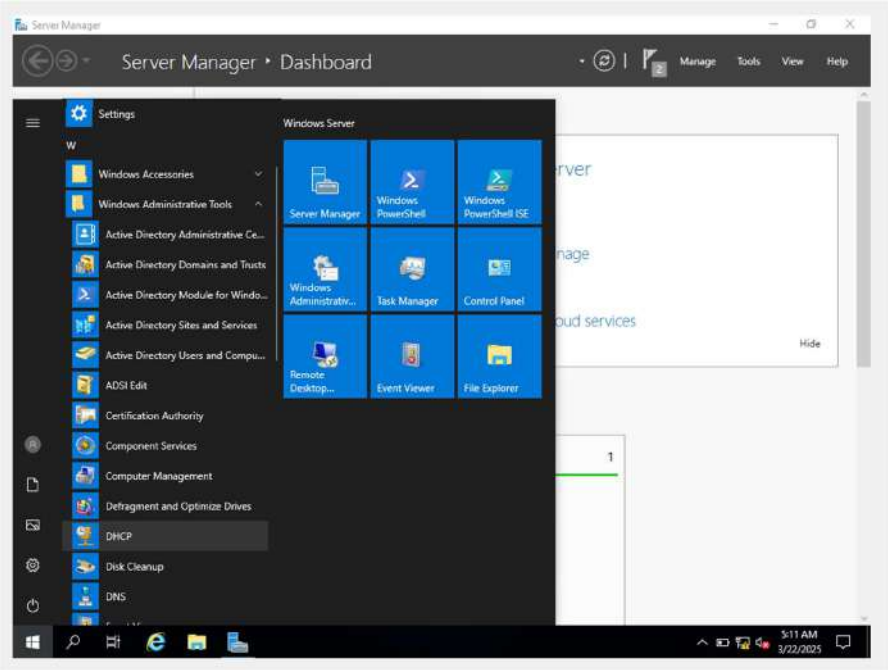
Click on **Commit**.



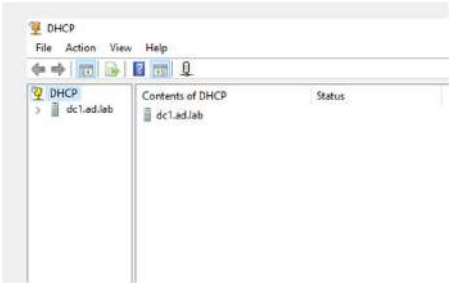
Click on **Close** to complete the installation.



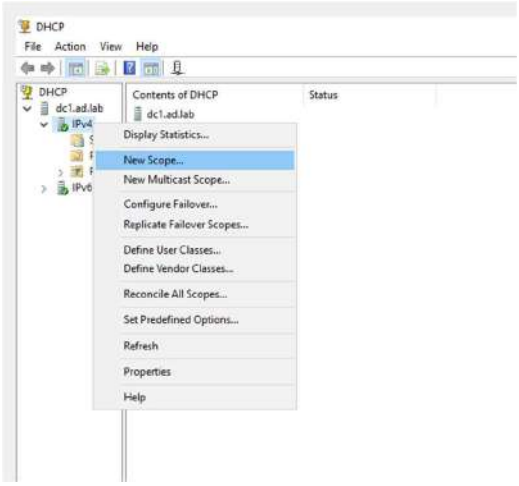
From the Start menu click on "Windows Administrative Tools" and then choose **DHCP**.



Expand the DHCP server (in my case **dc1.ad.lab**) dropdown on the left side of the window.

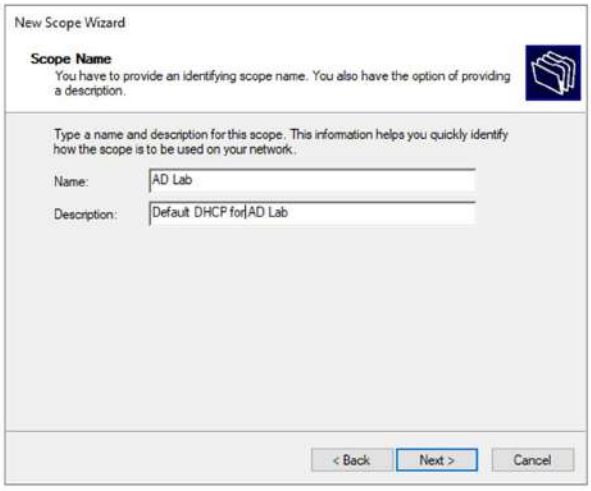


Right-click on **Ipv4**. Then select "New Scope". The scope defines the range of IP addresses that can be assigned to devices by the DHCP server.



Click Next.

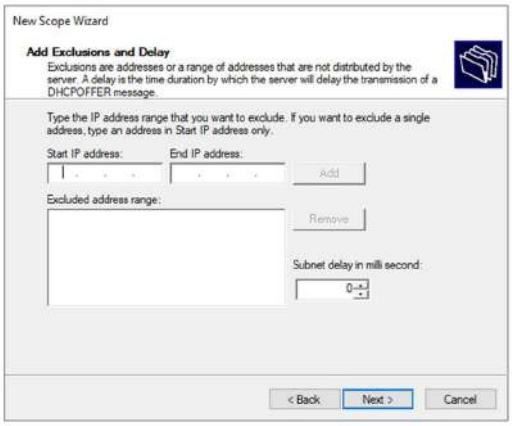
Enter a Name and Description for the new scope.



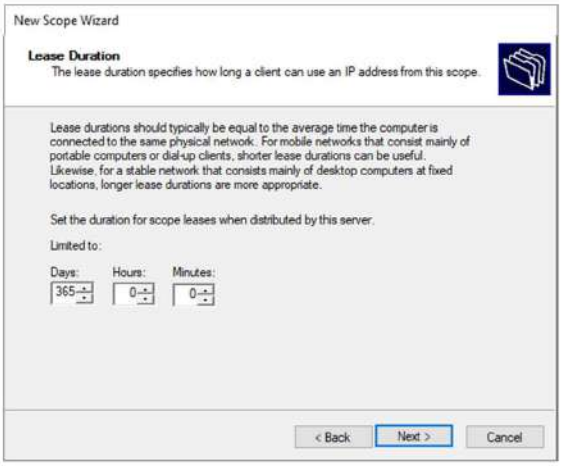
Enter the details as shown below.

Start IP address: **10.80.80.11**
End IP address: **10.80.80.253**
Length: **24**
Subnet mask: **255.255.255.0**

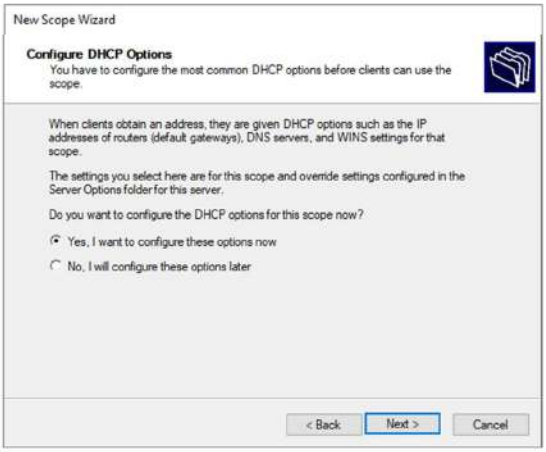
We don’t have any Exclusions (static IP assignment). Leave all the options empty and click on **Next**.



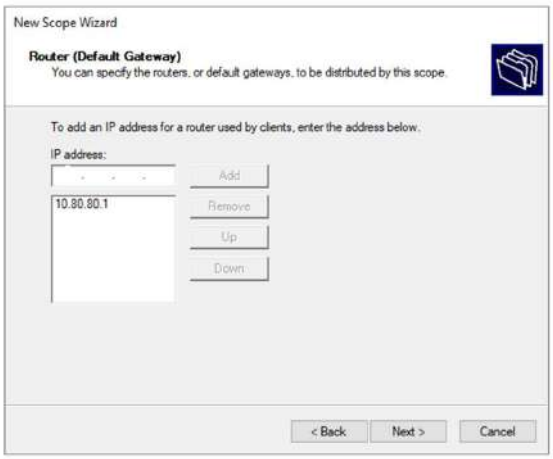
Increase the lease time to **365** days and click on **Next**.



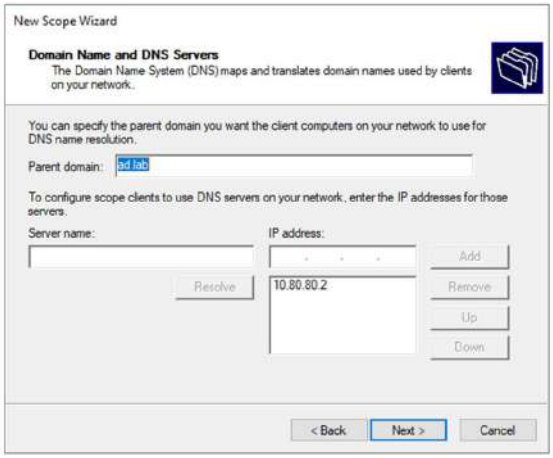
Select “<u>Yes, I want to configure these options now</u>” and click on **Next**.



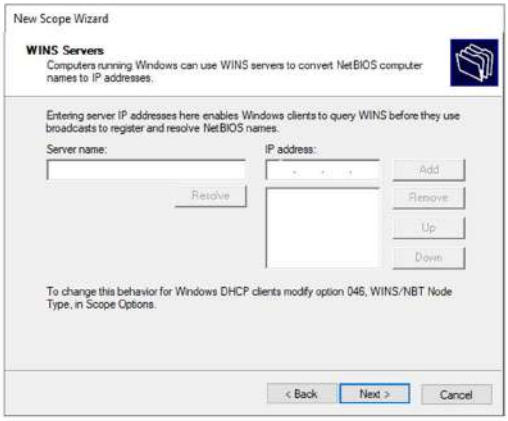
In the IP address field enter the default gateway for the **AD_LAB** interface (**10.80.80.1**) and then click on **Add**. Once added click on **Next**.



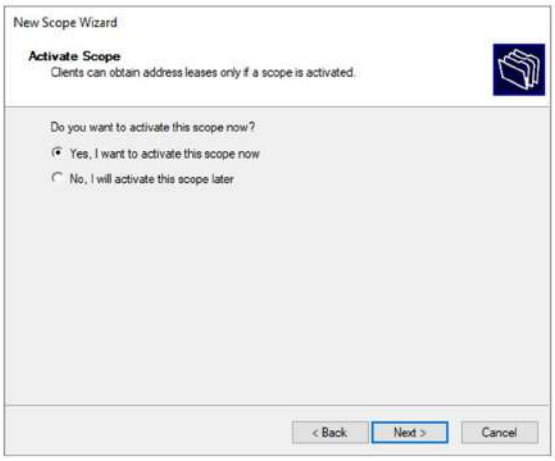
Click on **Next**.



We are not configuring a WINS Server for our environment so click on **Next**.



Select "Yes, I want to activate this scope now" and click on **Next**.

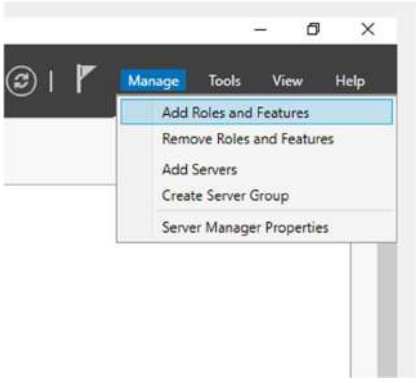


Click on **Finish**.

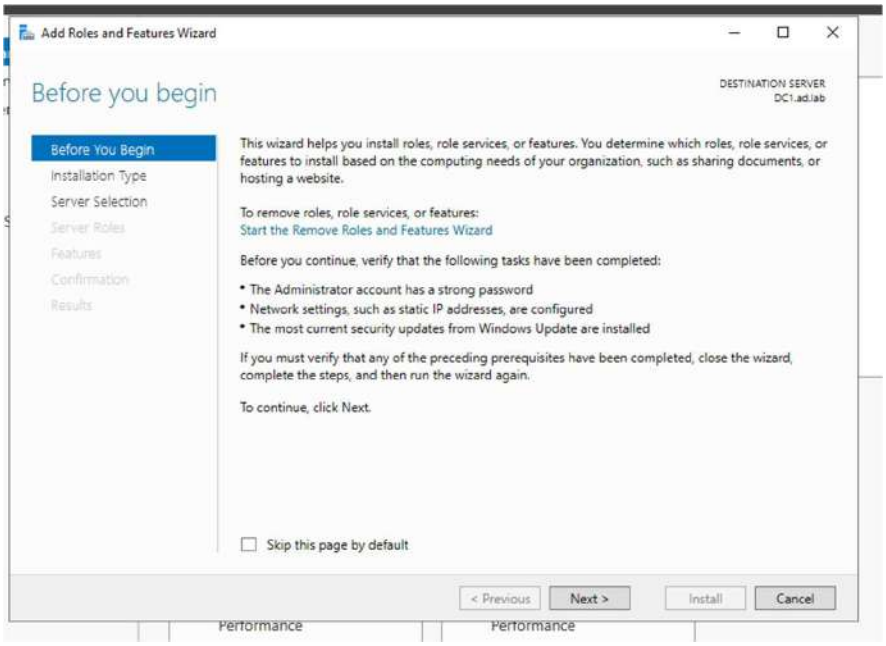
Domain Configuration

Certificate Service Installation

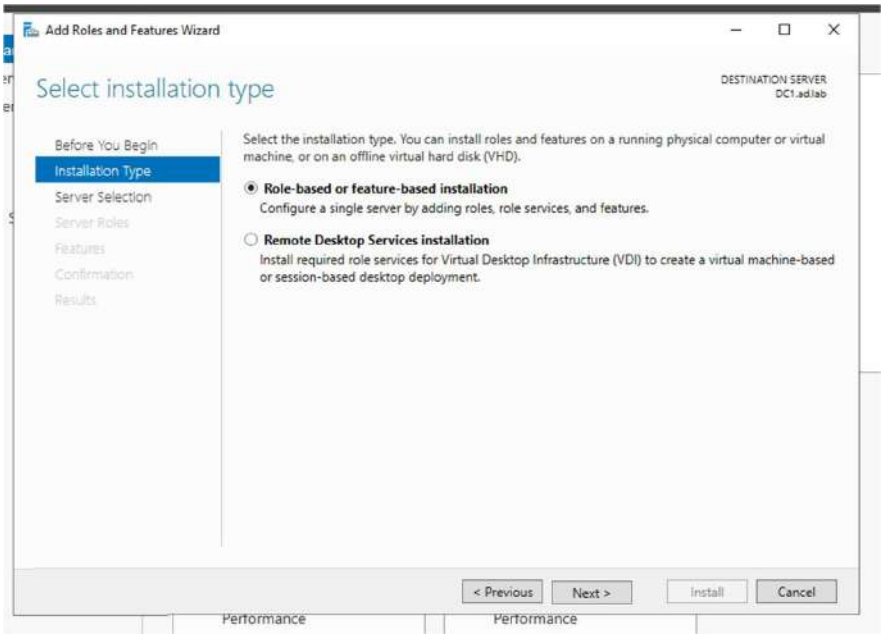
Select **Manage** from the top right corner of Server Manager and then select "Add Roles and Features".



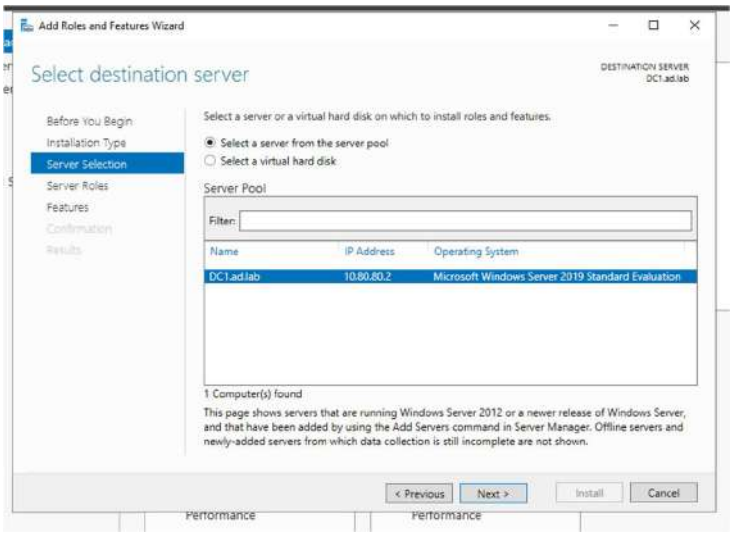
Click **Next**.



Click **Next**.

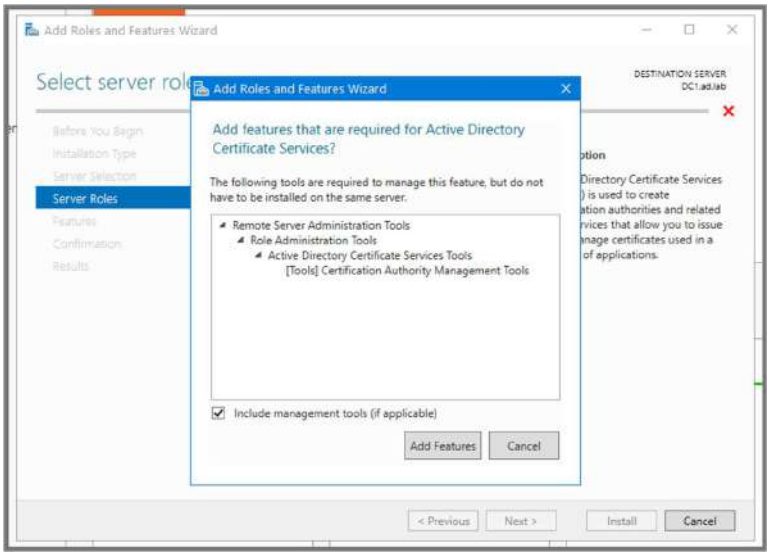


Click **Next**.

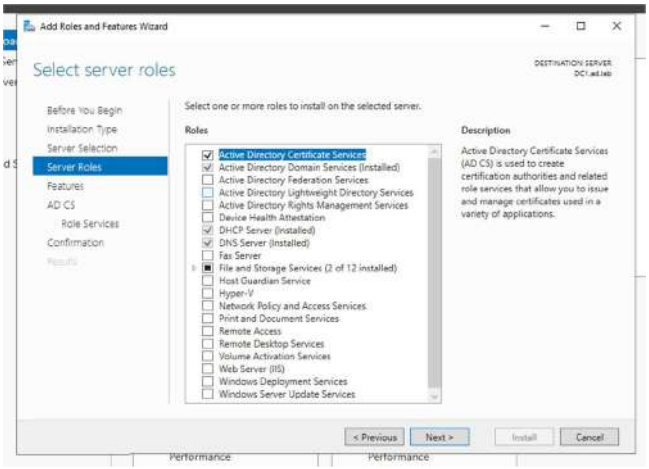


Enable "Active Directory Certificate Services".

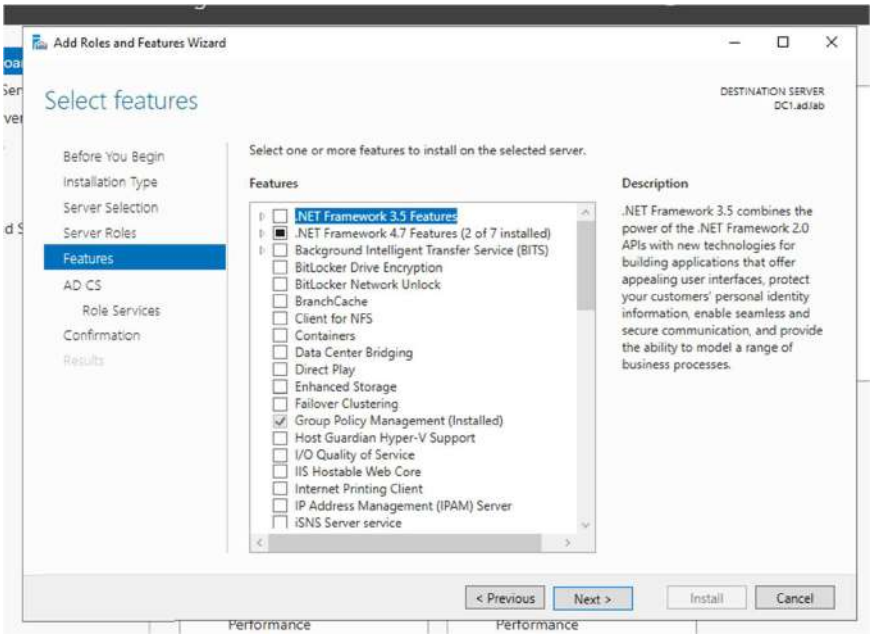
Click on **Add Features**.



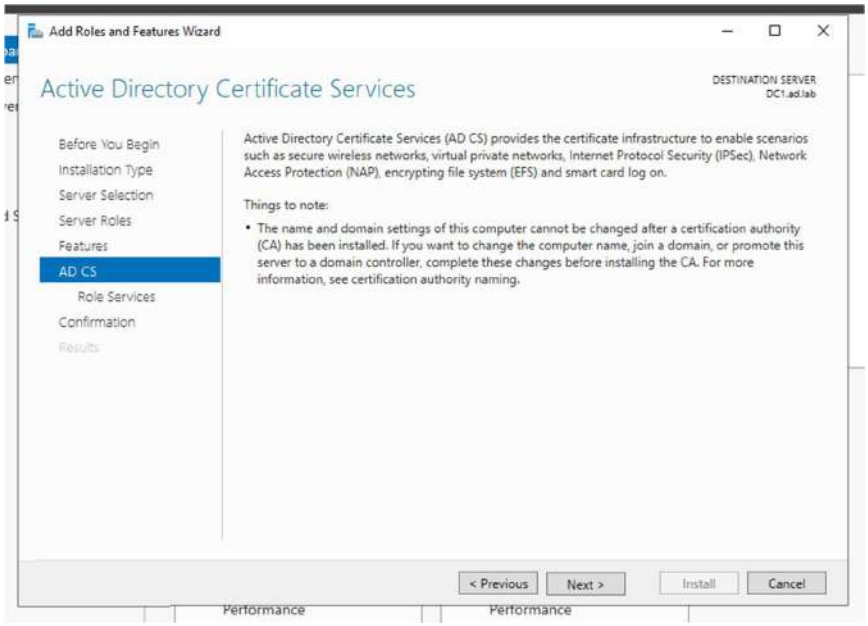
Click **Next**.



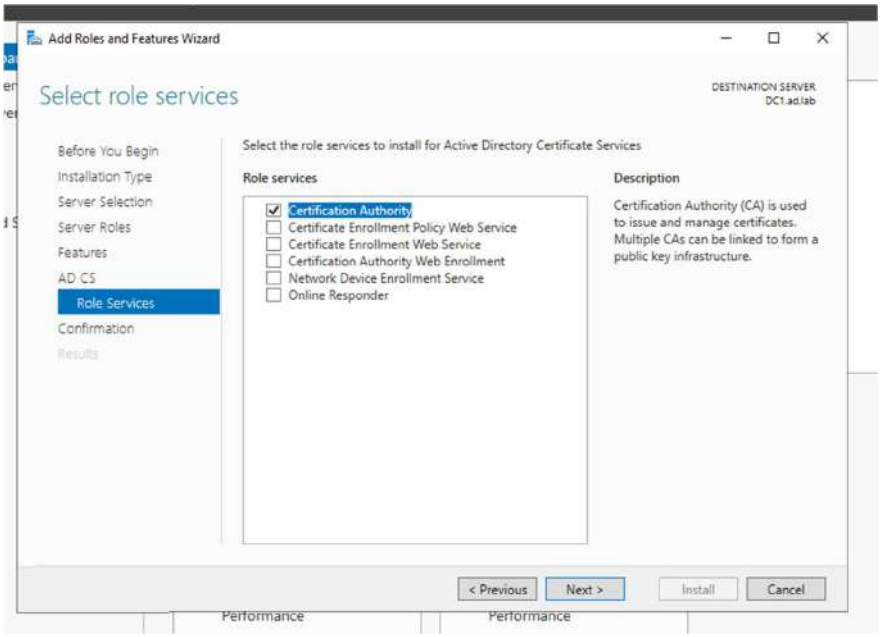
Click **Next**.



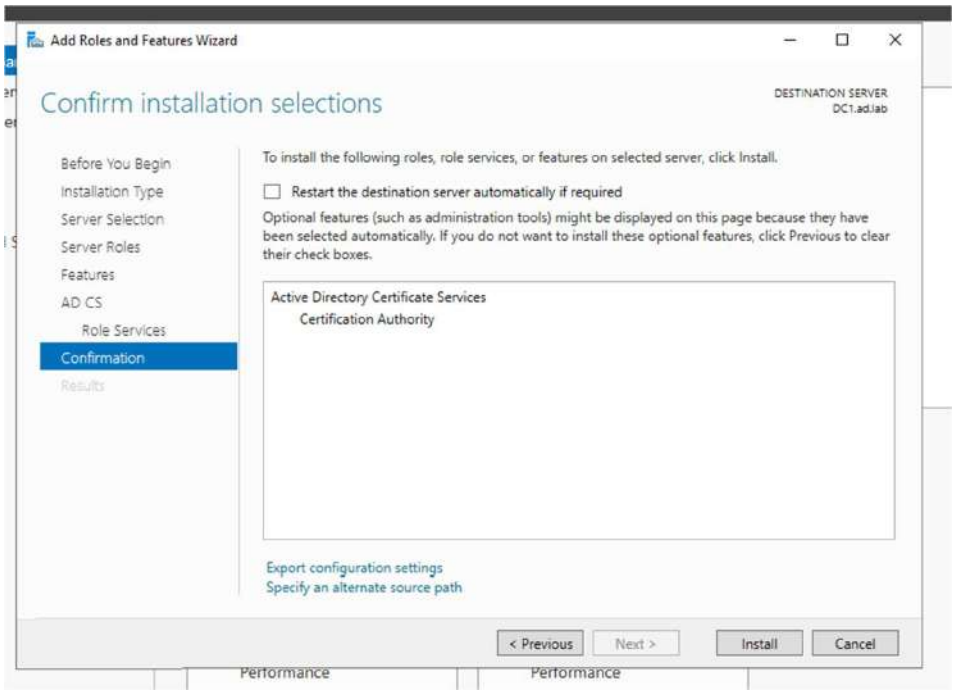
Click **Next**.



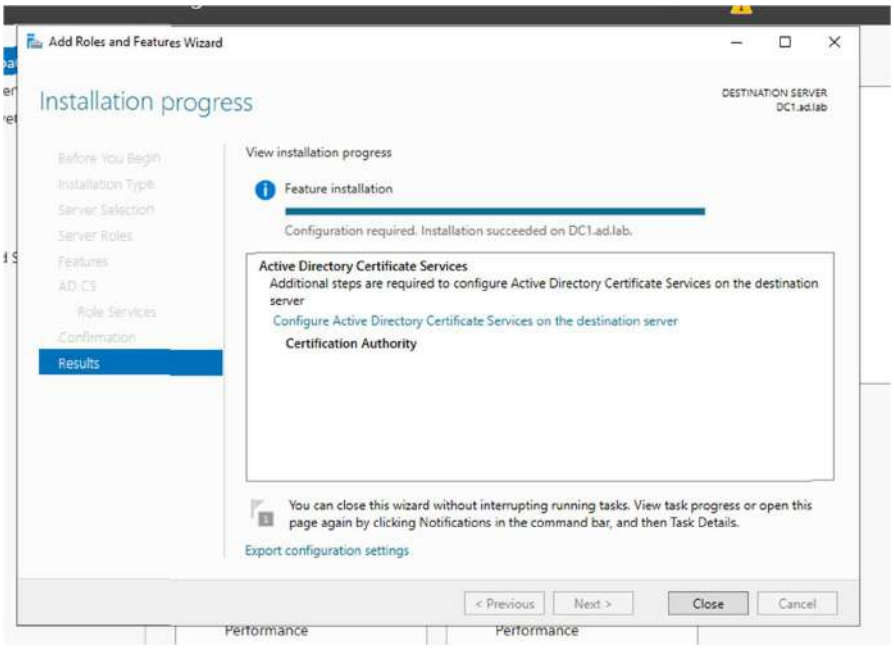
Enable "Certificate Authority". Click on **Next** to continue.



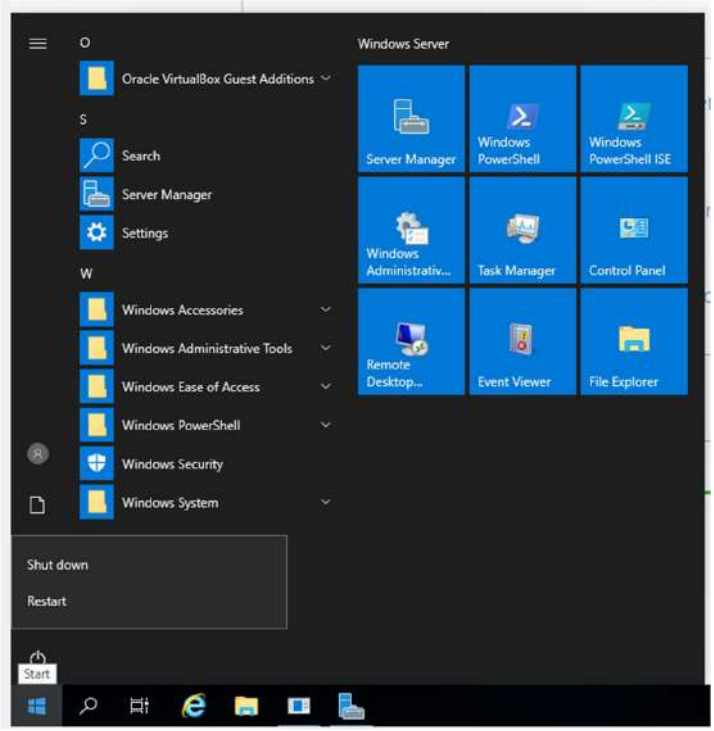
Click on **Install** to start the setup.



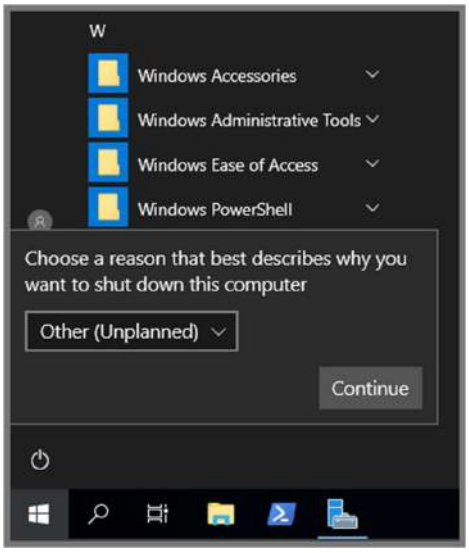
Click on **close** after installation.



After the installation is complete the server has to be restarted. Open the Start Menu, click on the Power icon and then select **Restart**.

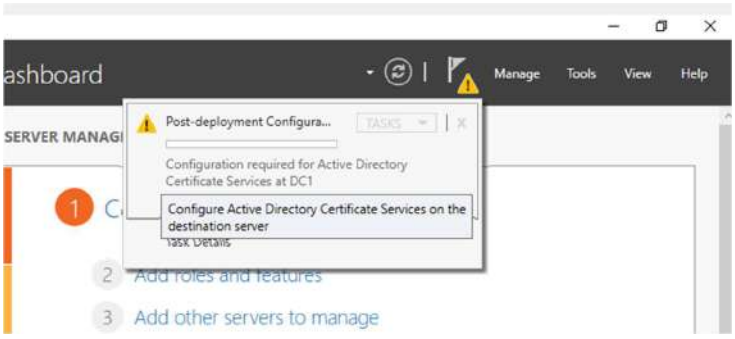


Click on **Continue** to restart the system.

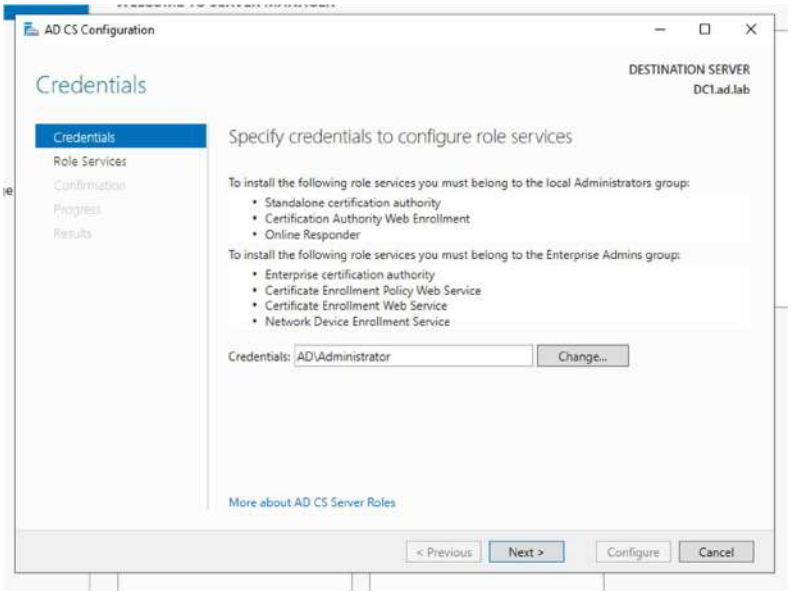


Certificate Service Configuration

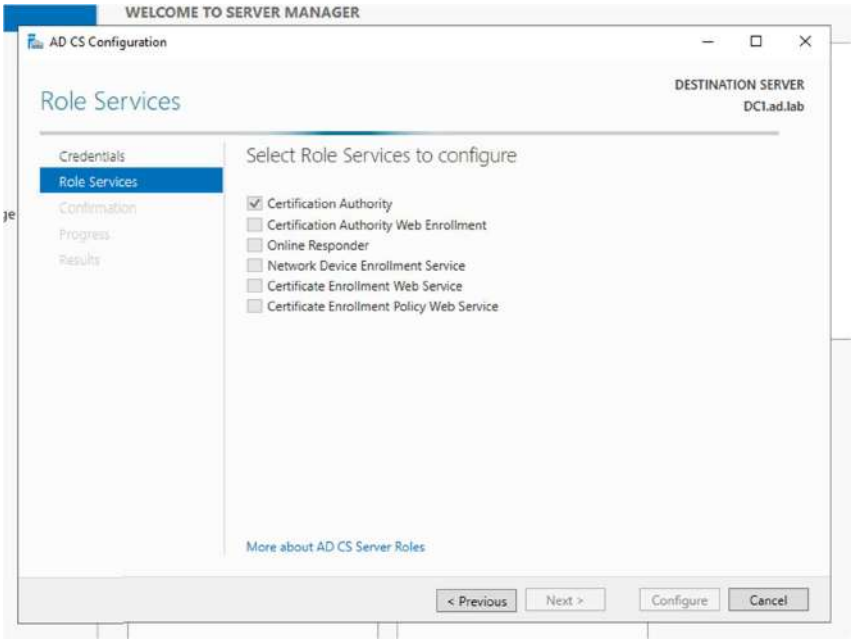
After the restart once Server Manager loads. Click on the Flag icon on the top right side and select "Configure Active Directory Certificate Services"



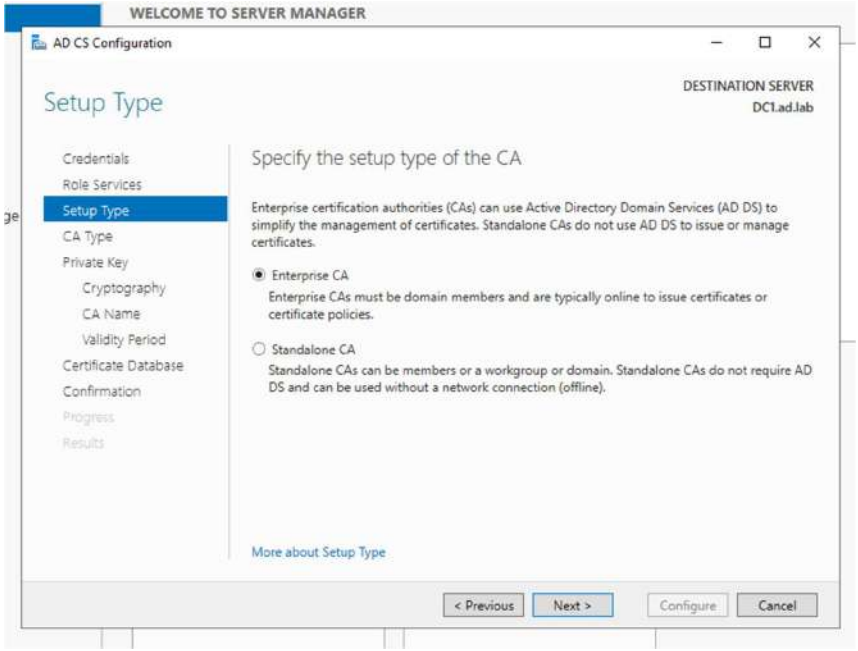
Click on **Next**.



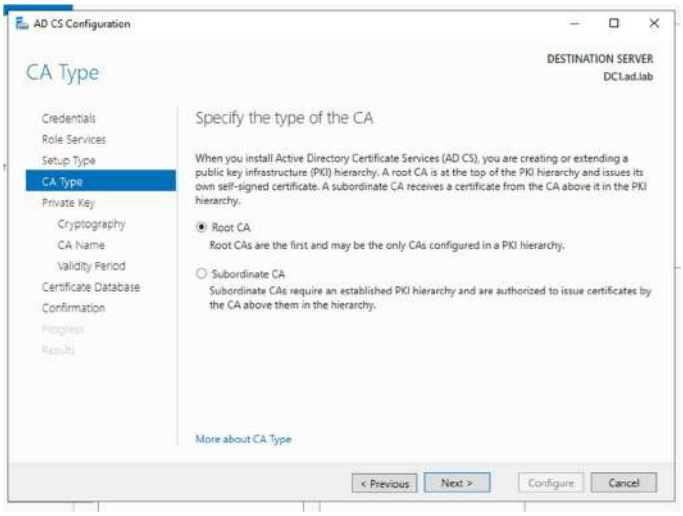
Enable "Certification Authority" and click on **Next**.



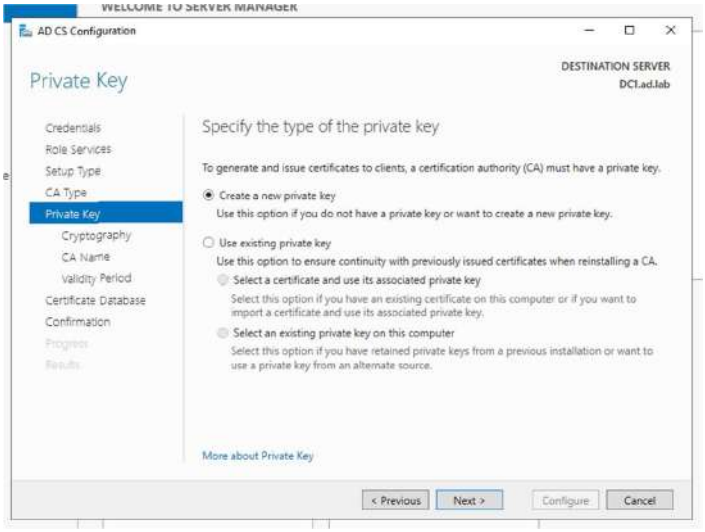
Click on **Next**.



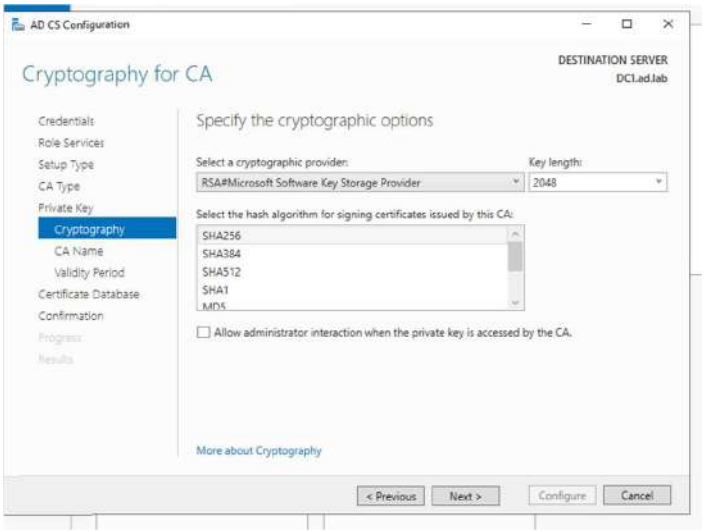
Click on **Next**.



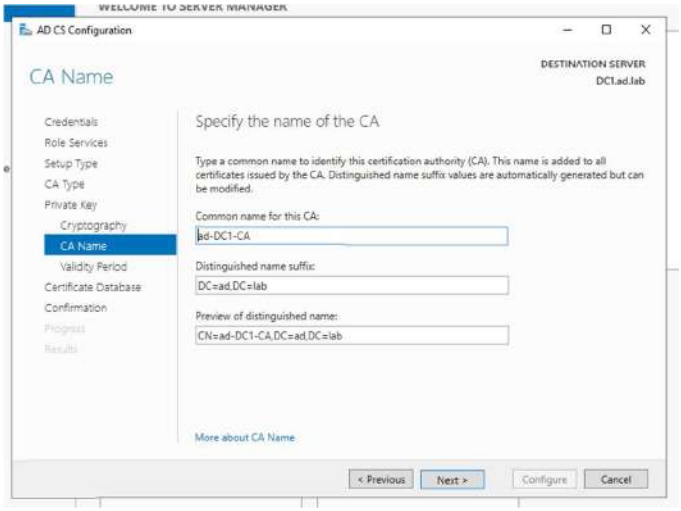
Click on **Next**.



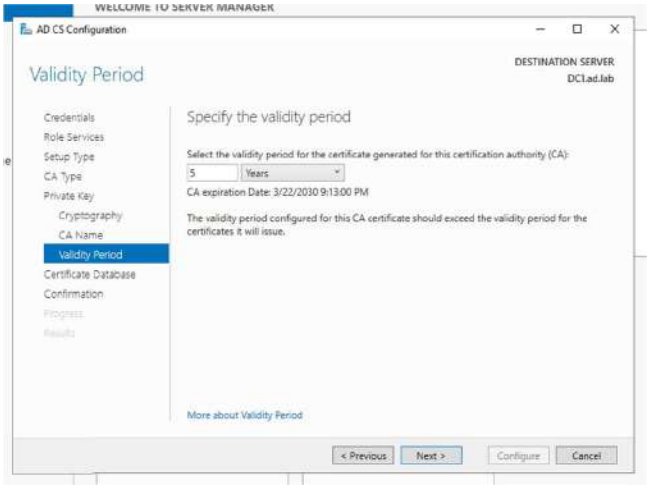
Click on **Next**.



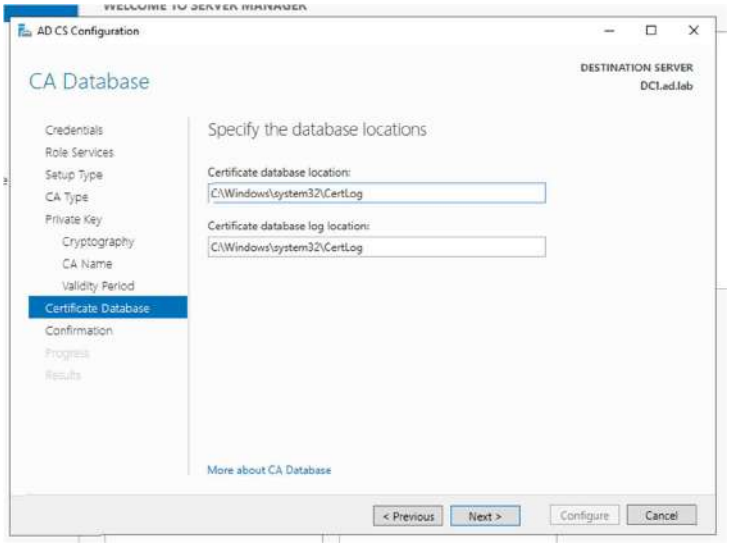
Click on **Next**.



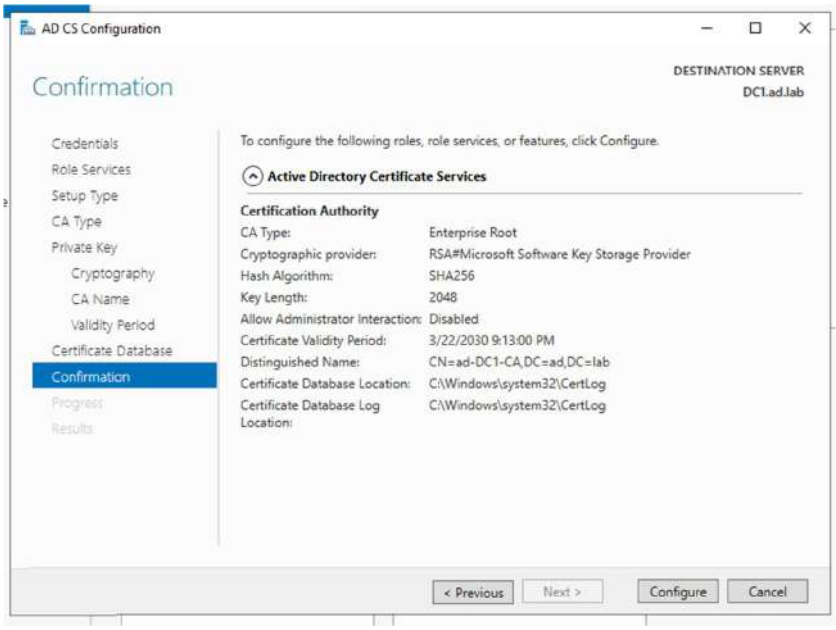
Click on **Next**.



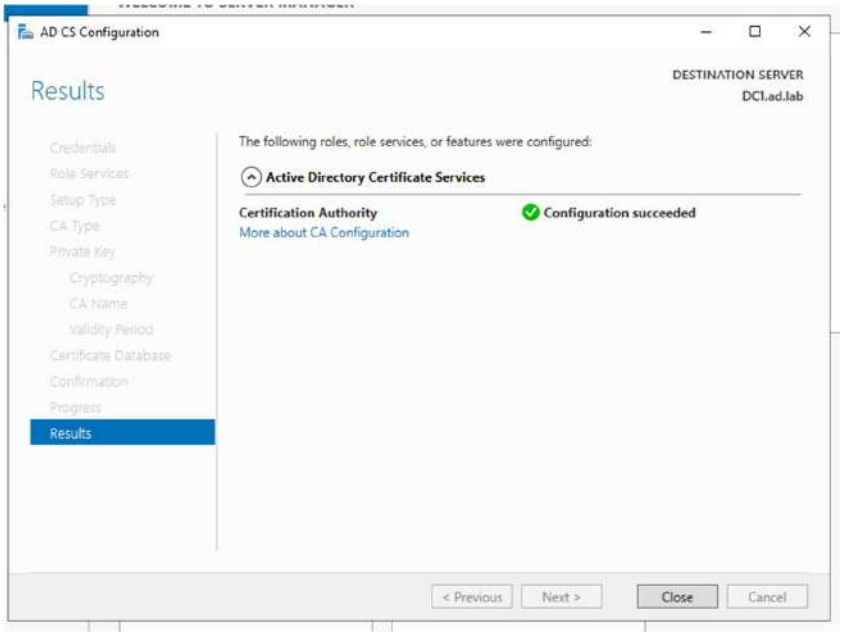
Click on **Next**.



Click on **Configure** to save the changes.



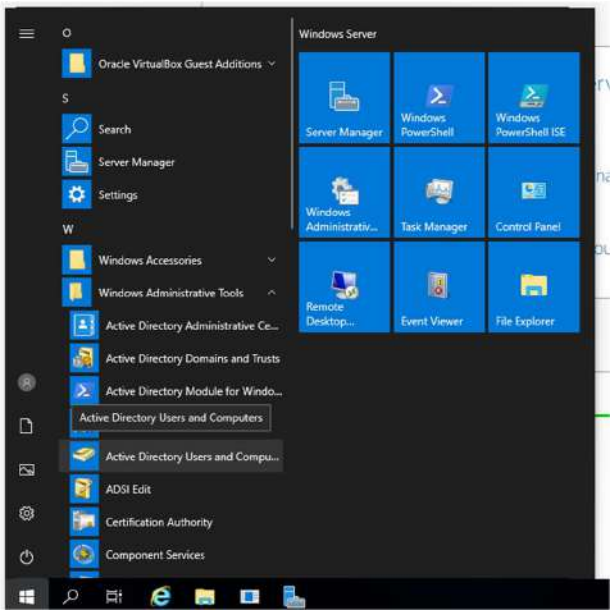
Click on **Close**.



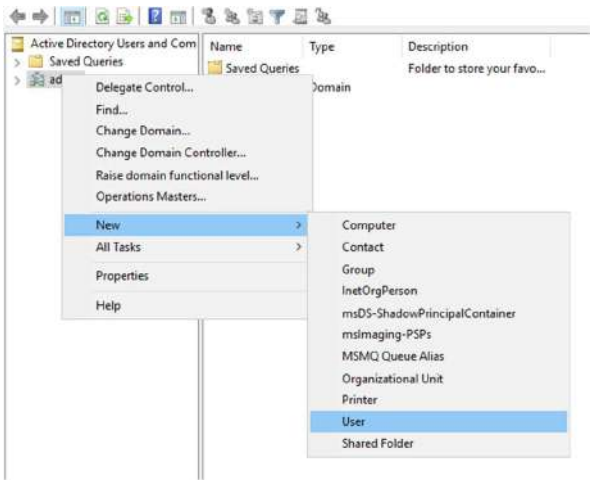
User Configuration

AD Admin Setup

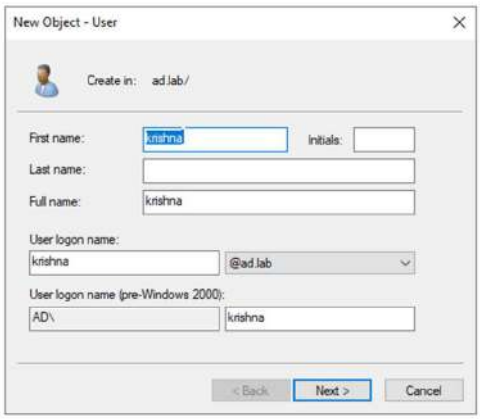
Open the Start menu click on "Windows Administrative Tools" and then select **Active Directory Users and Computers**.



Right-click on the domain name (in my case **ad.lab**) in the sidebar. Then select **New -> User**.

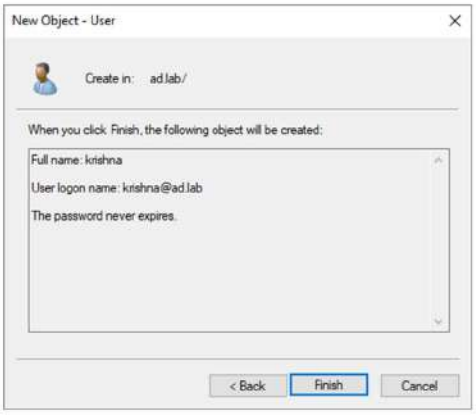


Enter the First Name, Last Name and User logon name for the new user. This user will be the **Administrator** for the Domain Controller.

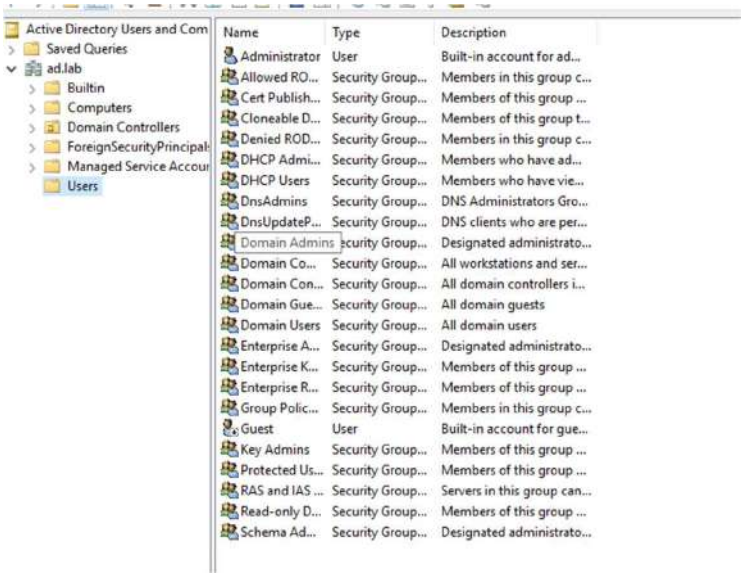


Enter the Password for the user. Uncheck all options leaving "Password never expires". Click on **Next** to create the user.

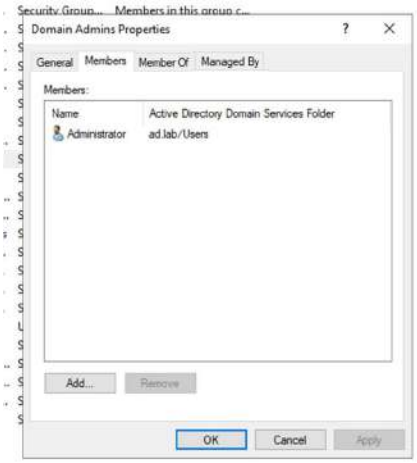
Click on **Finish.**



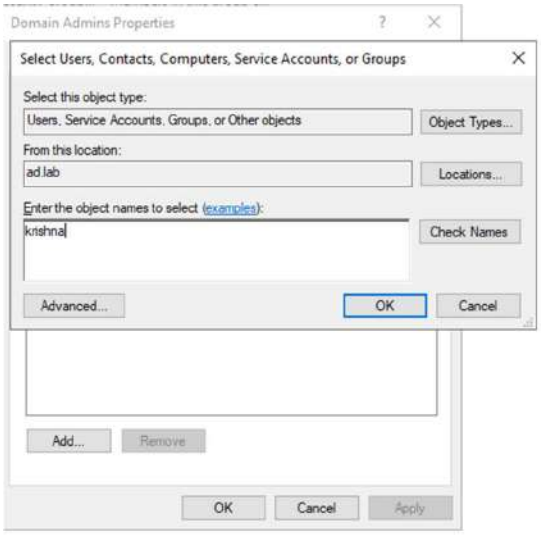
Expand the dropdown on the domain name from the sidebar. Click on **Users**. Then double-click on "Domain Admins".



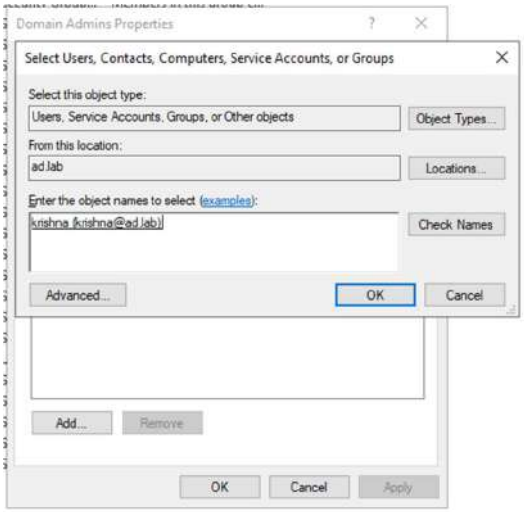
Go to **Members -> Add**.



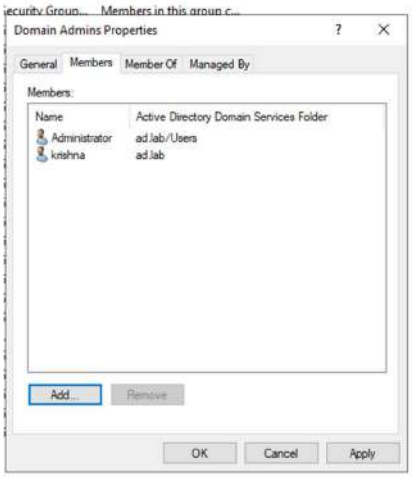
Enter the name of the user and check on **Check Names**.



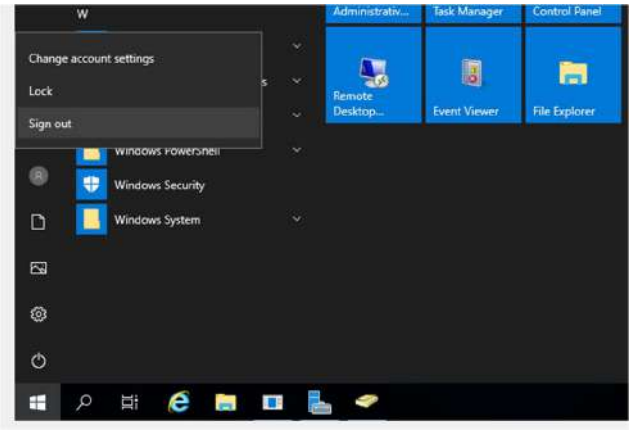
Click on **OK**.



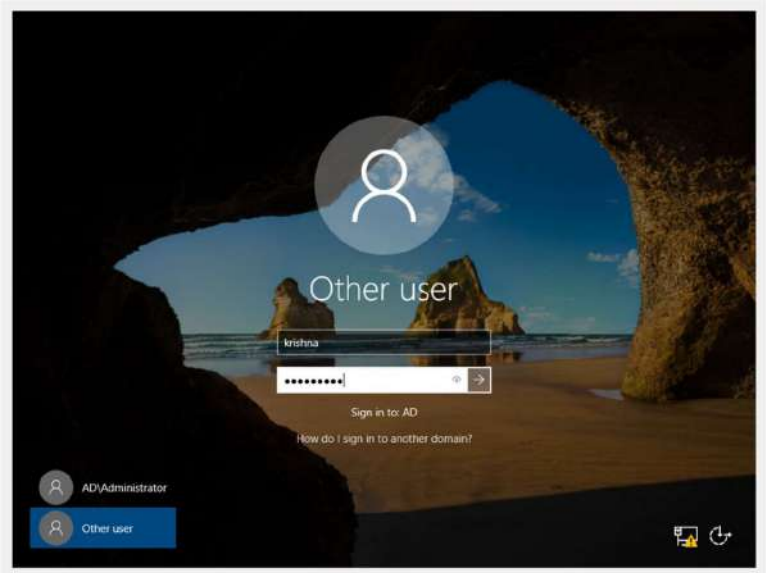
Click on **Apply** then **OK** to persist the changes.



Open the Start menu and then click on the user logo and then select **Sign out**.

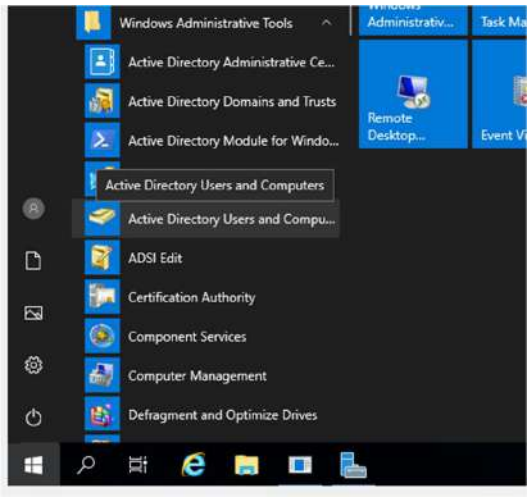


From the login screen select "Other user". Then enter the login name and password that was configured for your domain administrator.

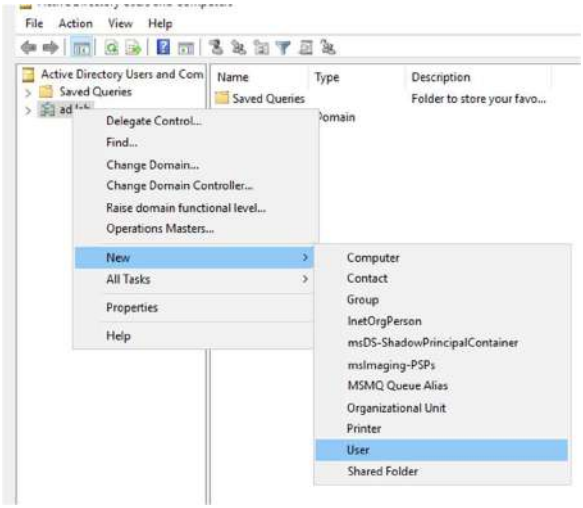


AD User 1 Setup

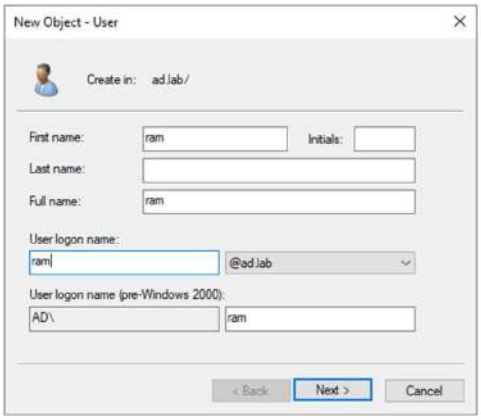
Open the Start menu. Select "Windows Administrative Tools" and then choose **Active Directory Users and Computers**.



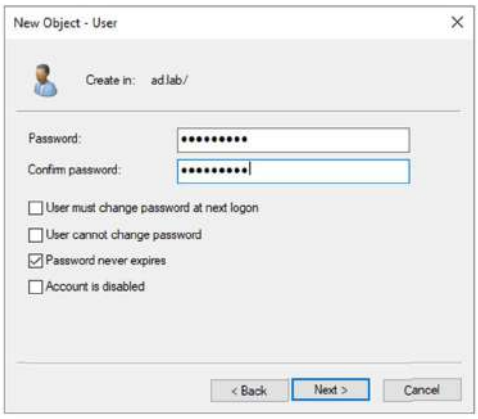
Right-click on the domain name from the sidebar. Select **New -> User**.



Enter the details for the user.



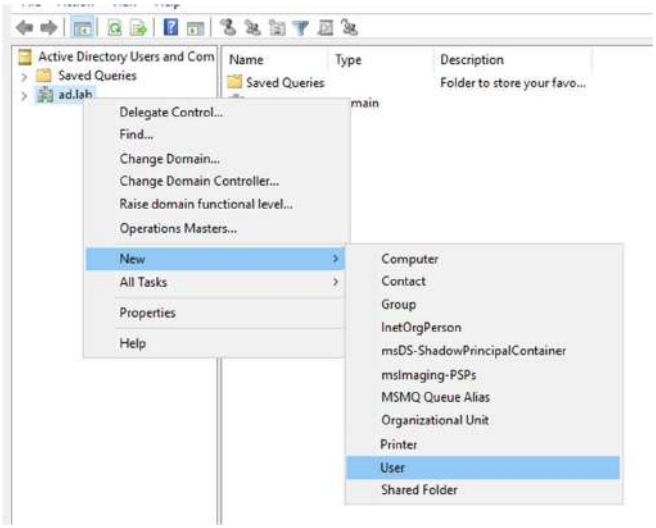
Give the user a password. Check the "User cannot change password" and "Password never expires" options. Click **Next** to create a user.

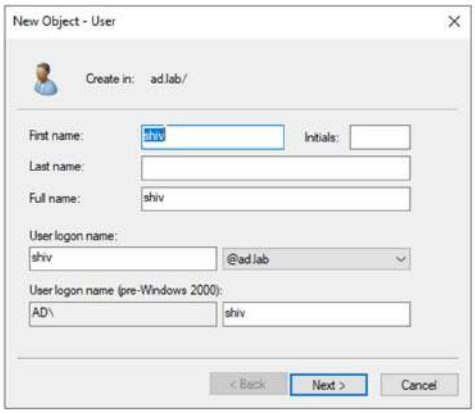


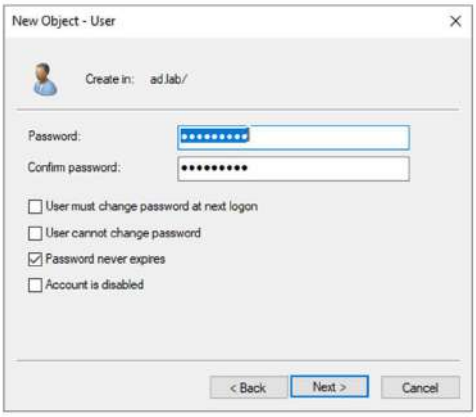
Click on **Finish.**

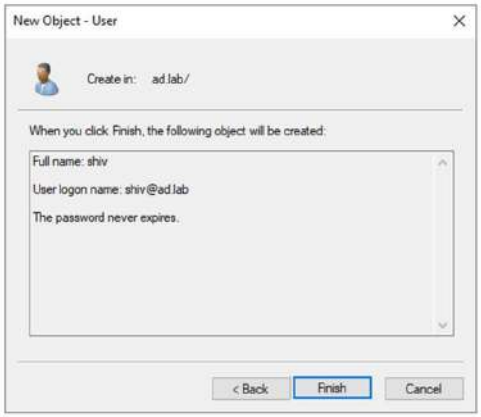
AD User 2 Setup

Follow the same steps as above to create a second AD User.







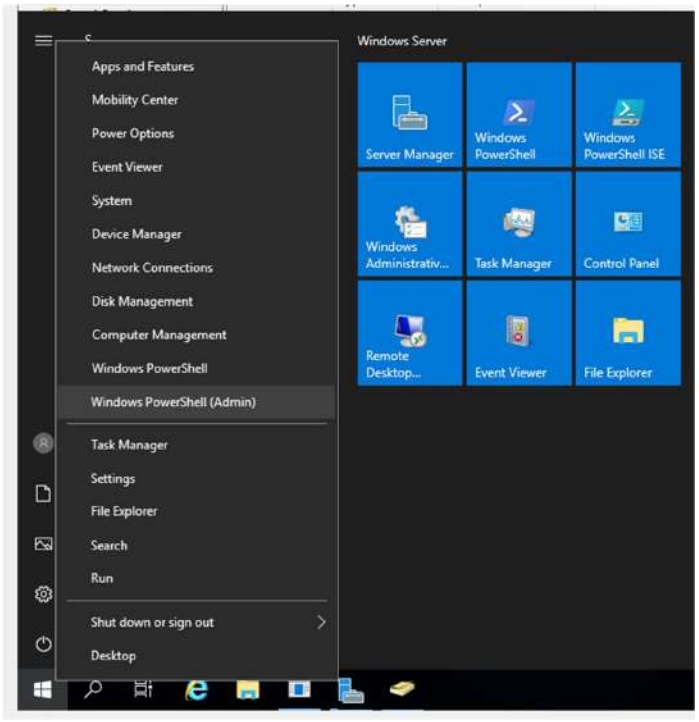


Making AD Lab Exploitable

To make the Active Directory Lab vulnerable we need to change some settings. We will use a PowerShell script and change so and Group Policies to achieve the desired result.

Running Vulnerable AD Script

Right-click on the Start menu and select **Windows PowerShell (Admin)**.



Run the following command:

Allows Execution of Scripts:

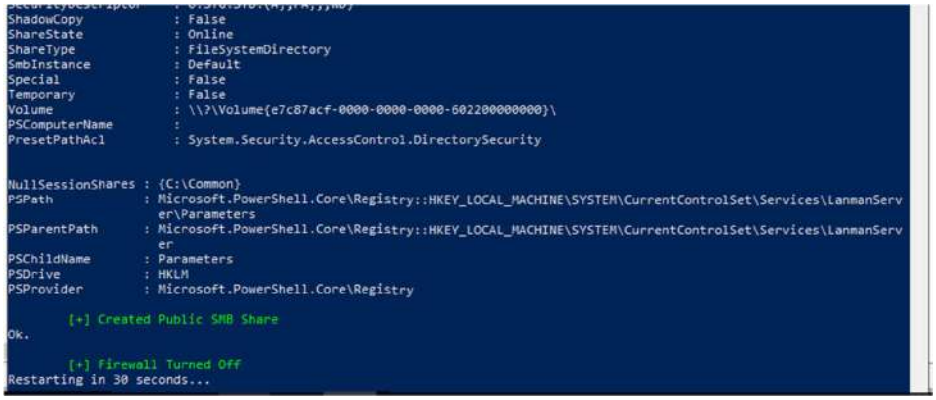
Set-ExecutionPolicy -ExecutionPolicy Bypass -Force

Download and Execute Script :

[System.Net.WebClient]::new().DownloadString('https://raw.githubusercontent.com/WaterExecution/vulnerable-AD-plus/master/vulnadplus.ps1') -replace 'change\.me', 'ad.lab' | Invoke-Expression

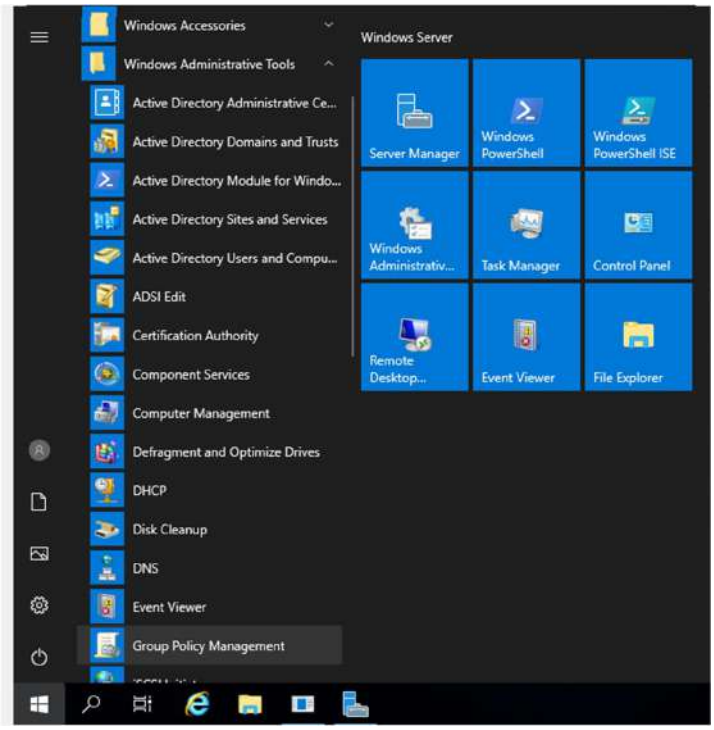
The above command constants of the following steps: **[System.Net.WebClient]::new().DownloadString()**: Downloads the Script
-replace: Change string present in the script
Invoke-Expression: Execute the Script

Once the script reaches the end. It will wait for 30 seconds and then restart the system.



Group Policy Configuration

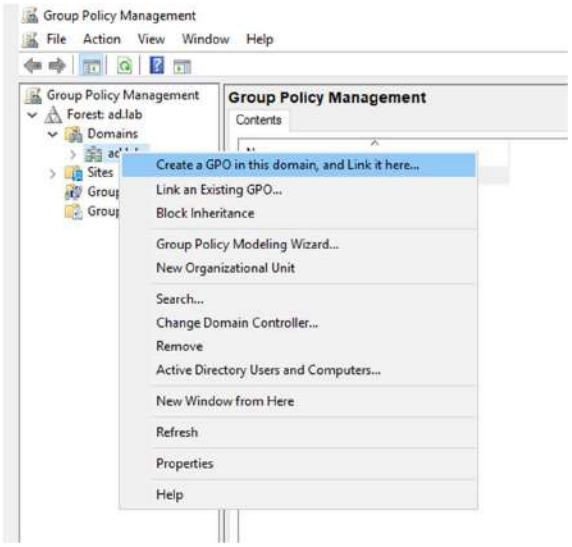
After the system restarts open the Start menu and click on "Windows Administrative Tools" then choose **Group Policy Management**.



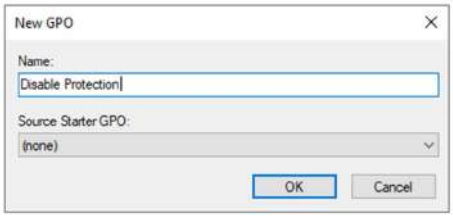
Expand "Forest" and then expand "Domains".

Disable Windows Defender and Firewall

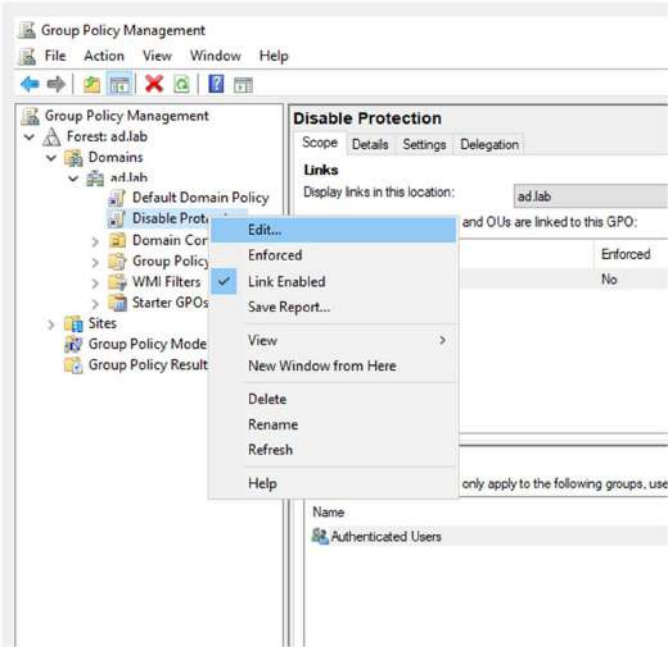
Right-click on the domain name. Select "Create a GPO in the domain and link here".



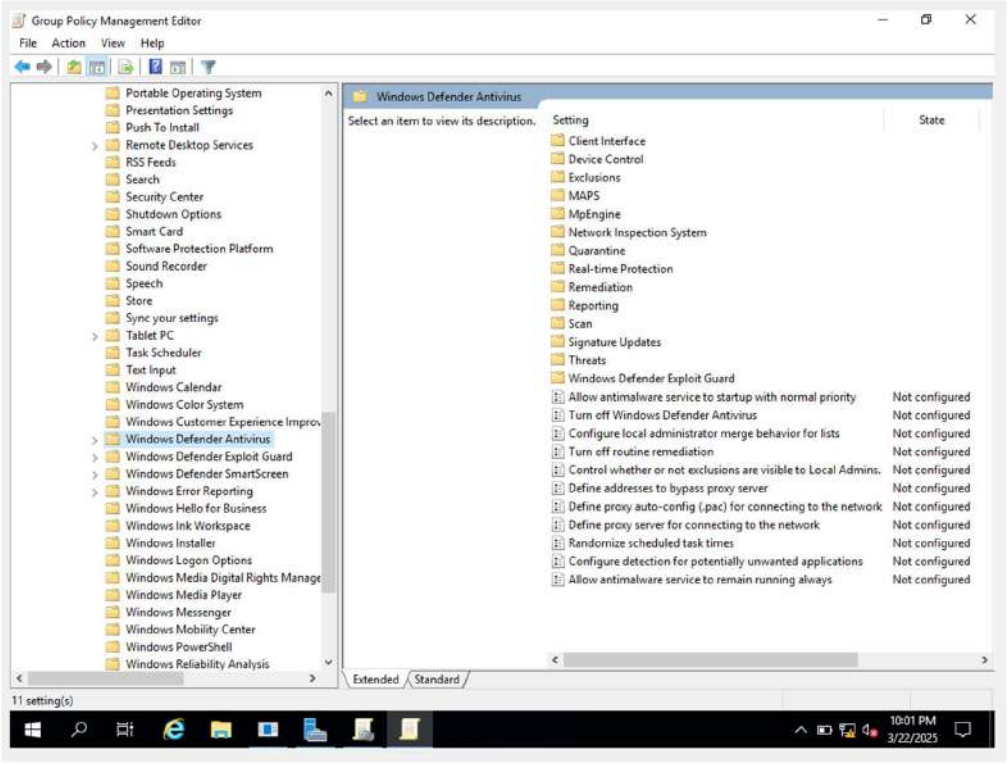
Give the GPO the name **Disable Protections**.



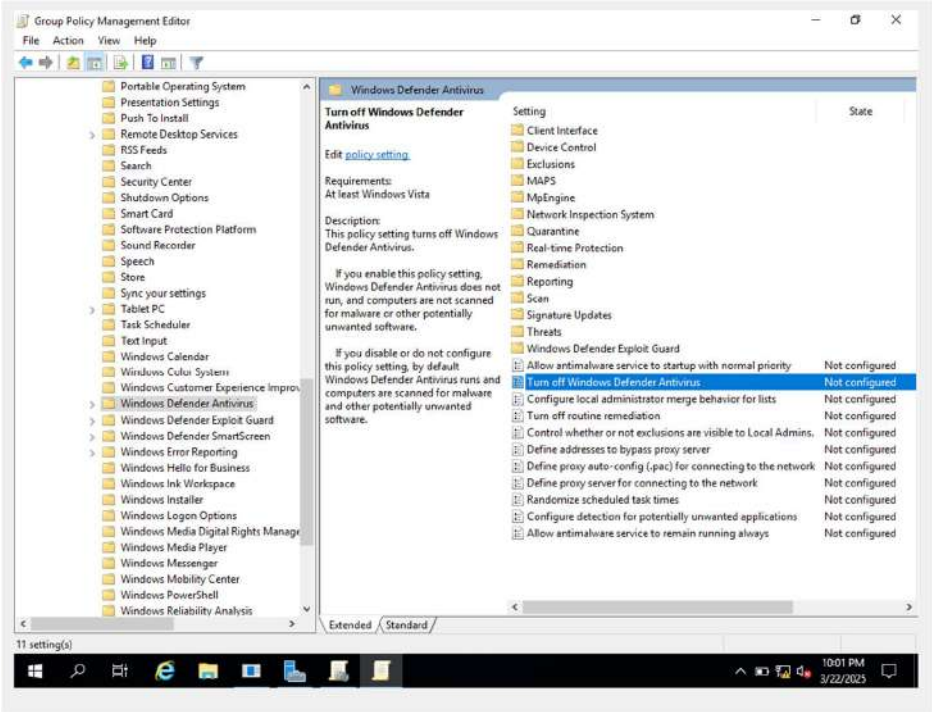
Expand the domain name. Right-click on "Disable Protections" and choose **Edit**.



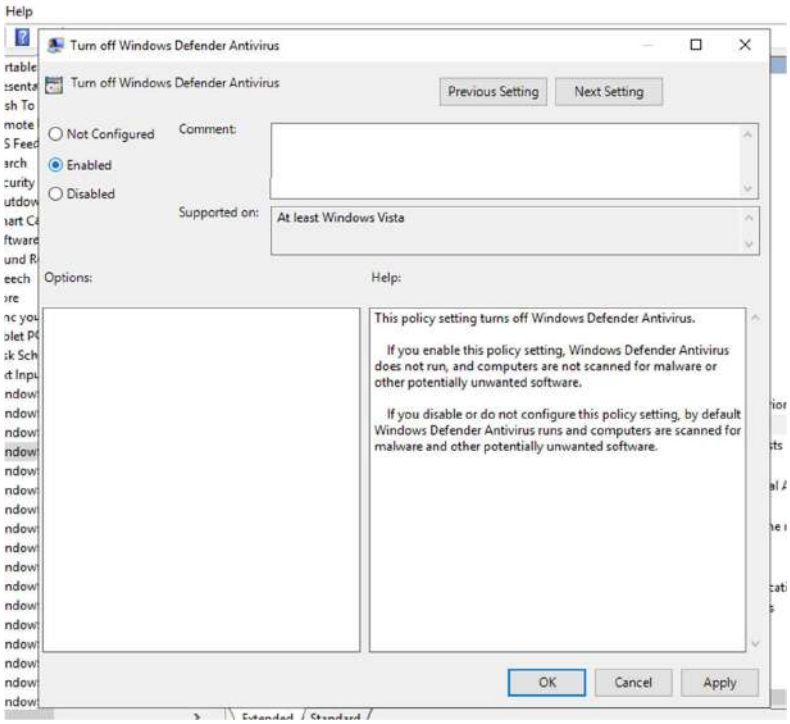
This will open the Group Policy Management Editor. From the sidebar go to the following folder: **Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Defender Antivirus**.



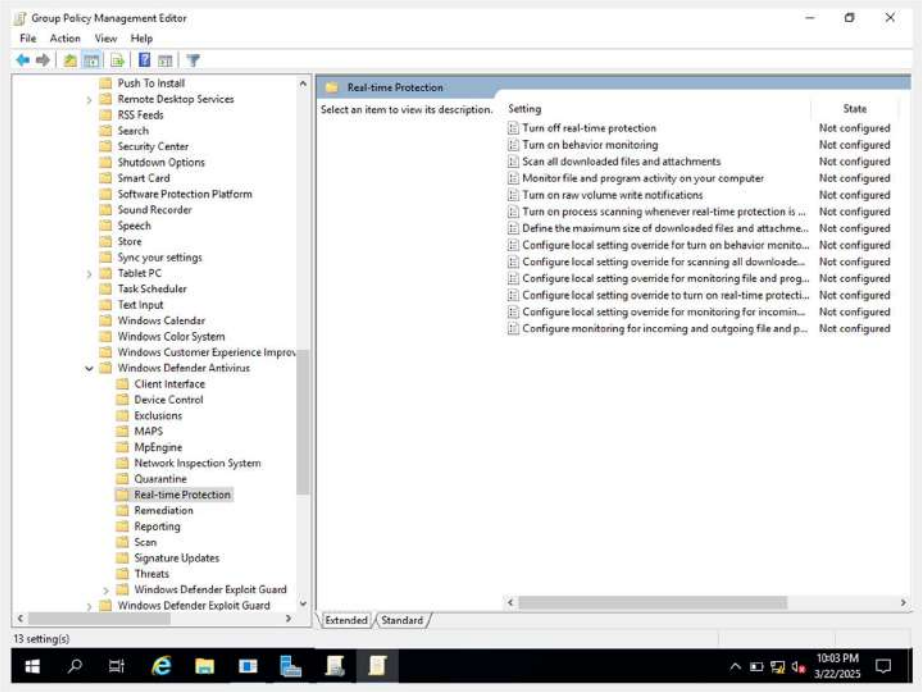
Select "Windows Defender Antivirus". From the right side select "Turn off Windows Defender Antivirus" and click on **Edit policy setting**.



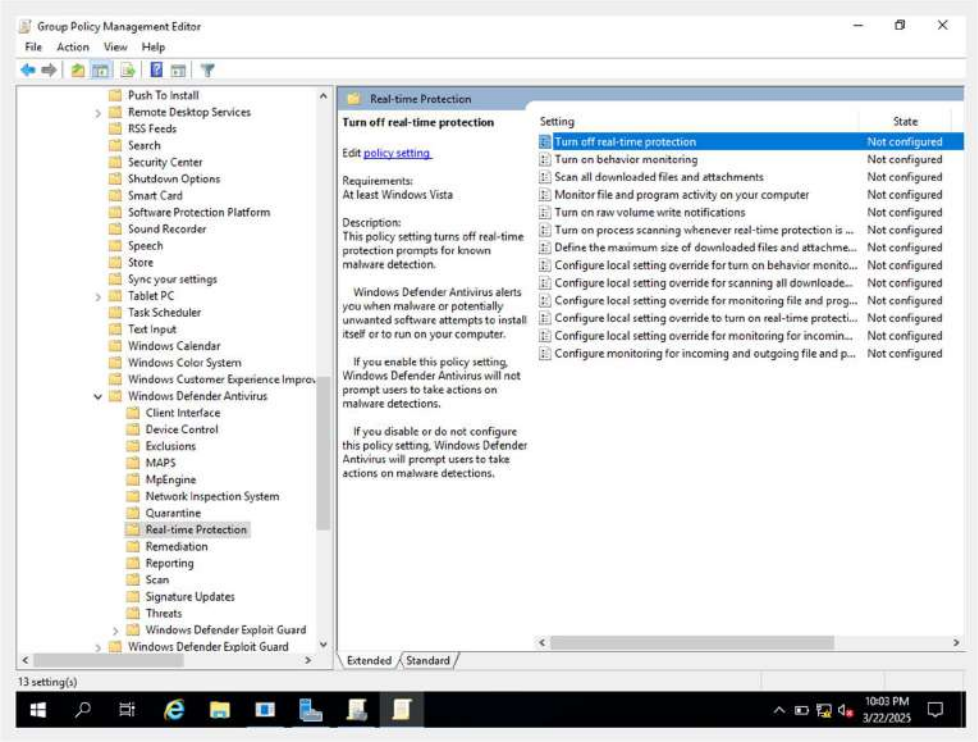
Set it to **Enabled**. Click on **Apply** then **OK** to save the changes.



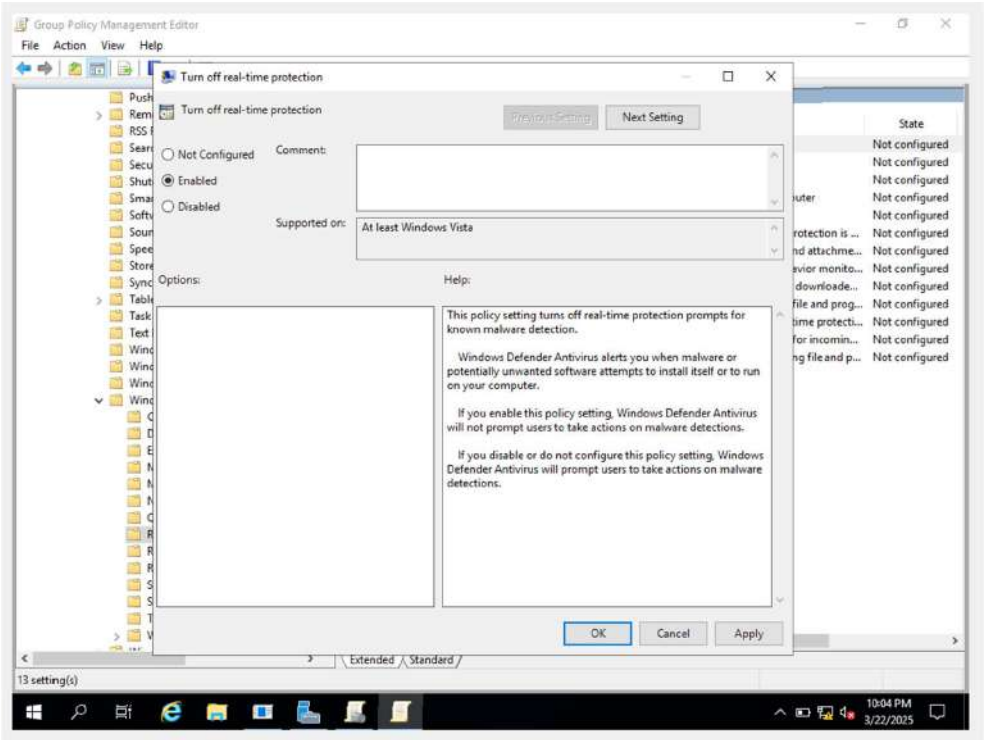
Double-click on **Real-time Protection**



Select “Turn off real-time protection” and then click on “Edit policy settings”

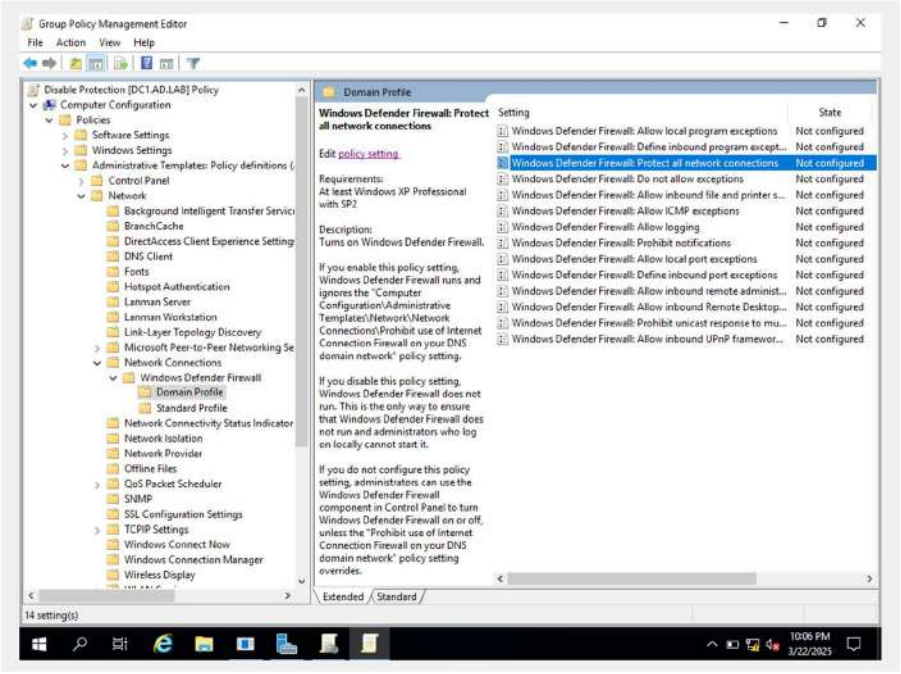


Set it to **Enabled**. Click on **Apply** then **OK** to save the changes.

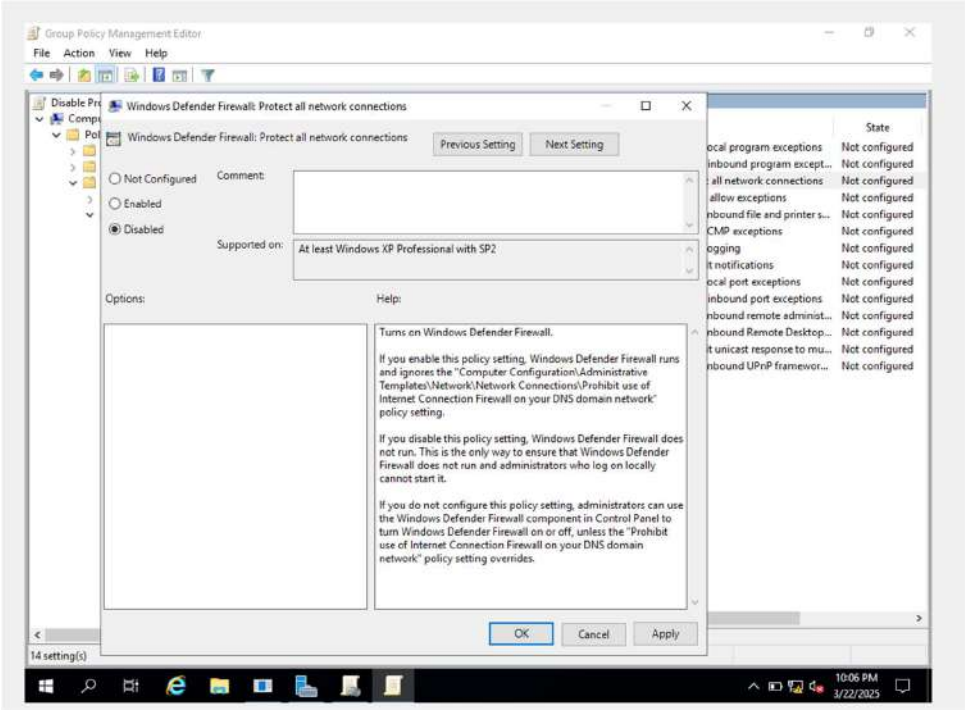


Expand the sidebar folders to the following: **Computer Configuration -> Policies -> Administrative Templates -> Network -> Network Connections -> Windows Defender Firewall -> Domain Profile**.

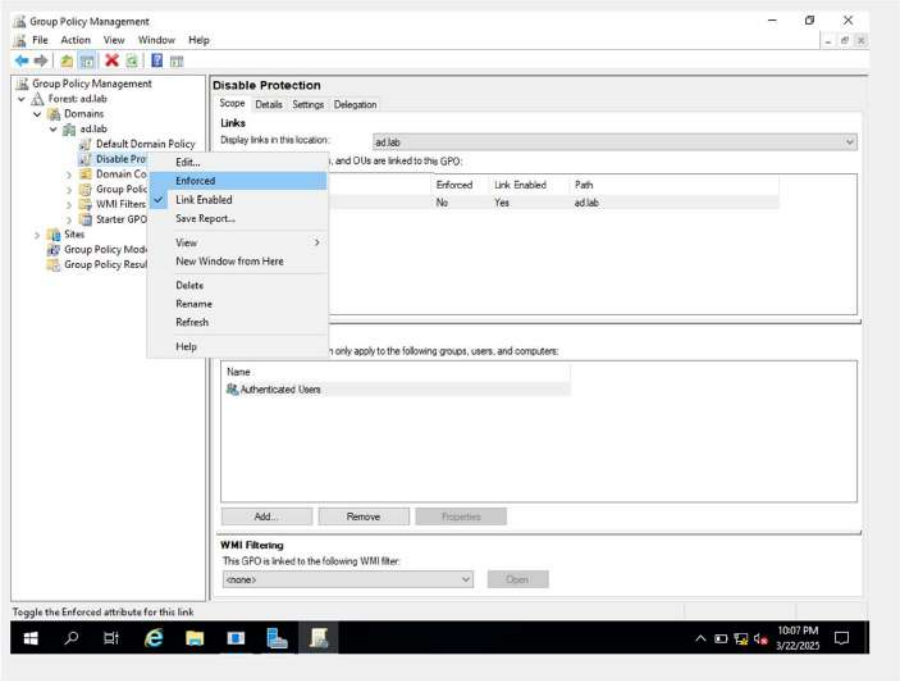
Select “Windows Defender Firewall: Protect all network connections”. Click on “Edit policy settings”.



Set it to **Disabled**. Click on **Apply** then **OK** to save the changes.

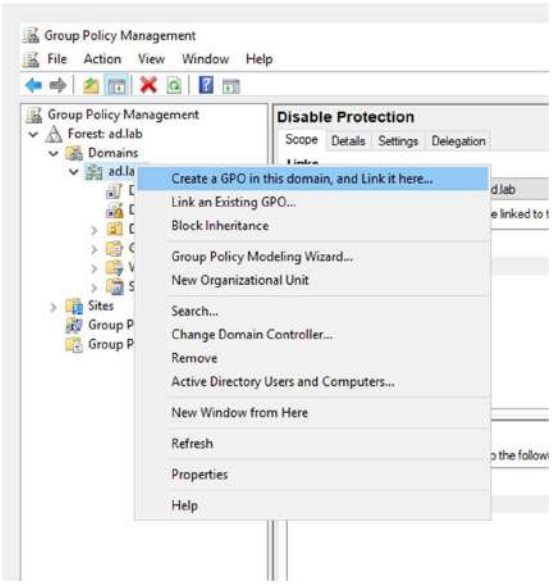


Close Group Policy Management Editor. From the sidebar of Group Policy Management right-click on “Disable Protections” and choose “Enforced”.

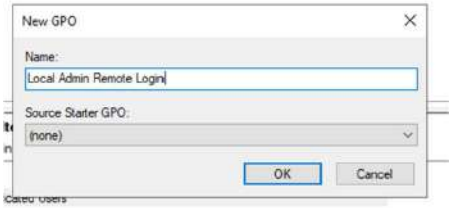


Enable Remote Login for Local Admins

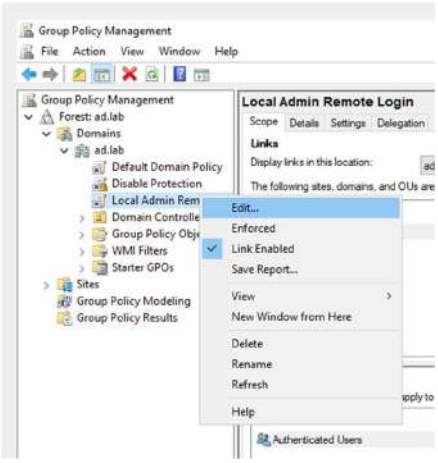
Right-click on the domain name. Select "Create a GPO in the domain and link here".



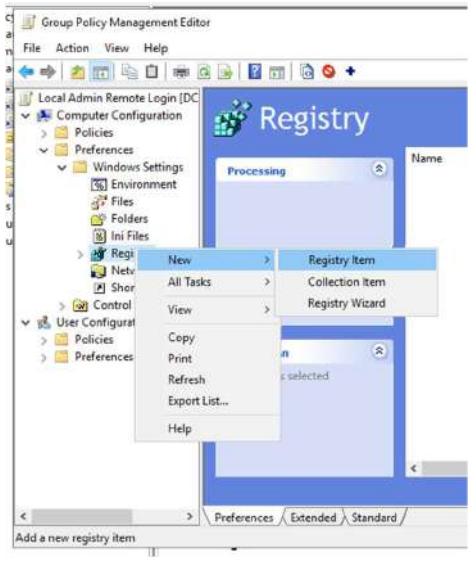
Give the GPO the name **Local Admin Remote Login**.



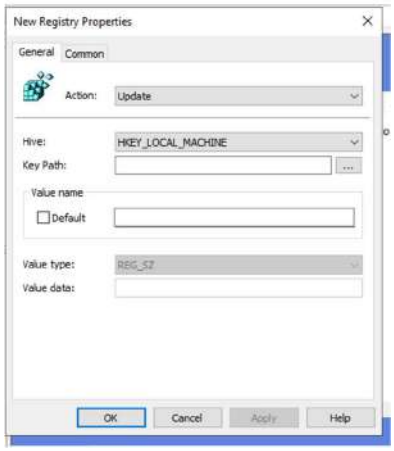
ight-click on "Local Admin Remote Login" and choose **Edit**.



Using the sidebar descend into **Computer Configuration -> Preferences -> Windows Settings -> Registry**. Then, right-click **Registry** and choose **New -> Registry Item**.



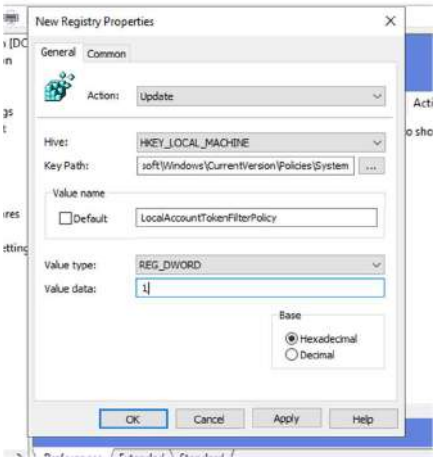
For the Hive field select **HKEY_LOCAL_MACHINE**. To fill the value in the "Key Path" field click on the **…** button.



In the window that opens up navigate to the following directory: **SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**

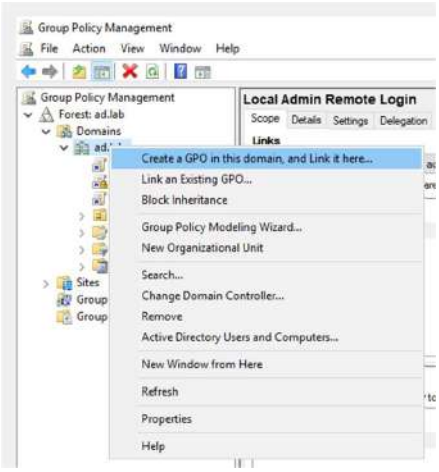
Thenenter the following for the remaining fields:
Value name: **LocalAccountTokenFilterPolicy**
Value type: **REG_DWORD**
Value data: **1**

Click on **Apply** then **OK**. Close Group Policy Management Editor.

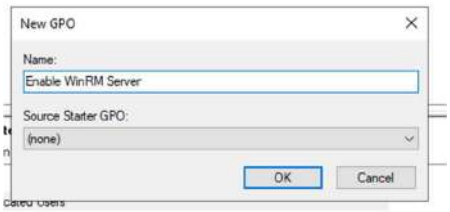


Enable WinRM Server

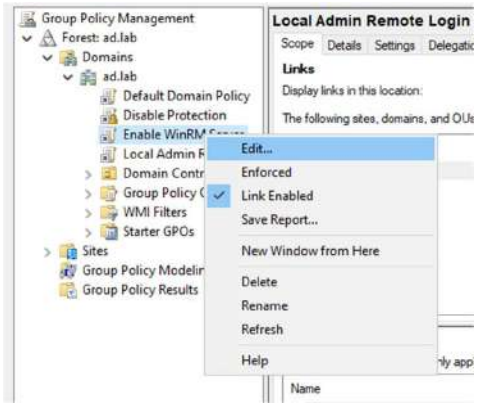
Right-click on the domain name. Select "Create a GPO in the domain and link here".



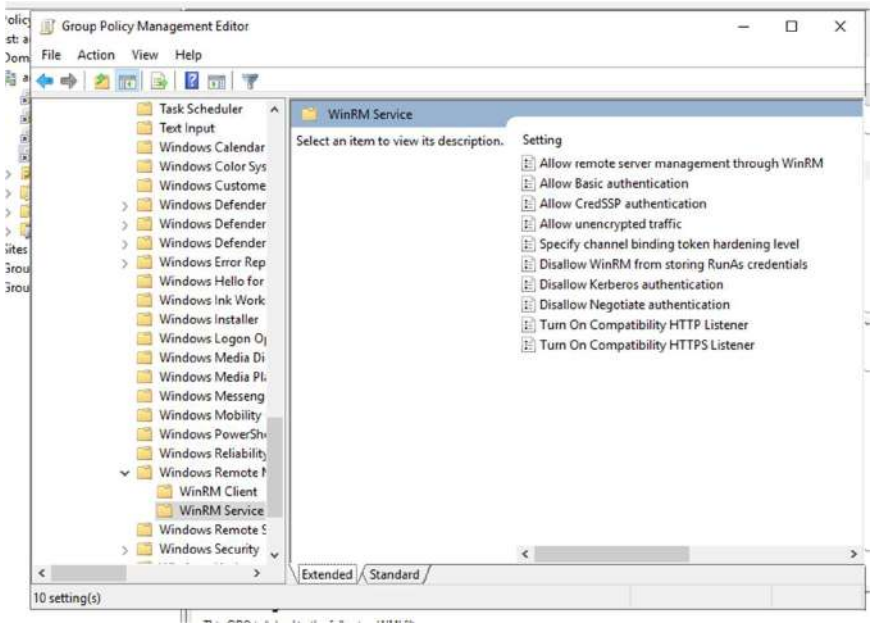
Give the GPO the name **Enable WinRM Server**.



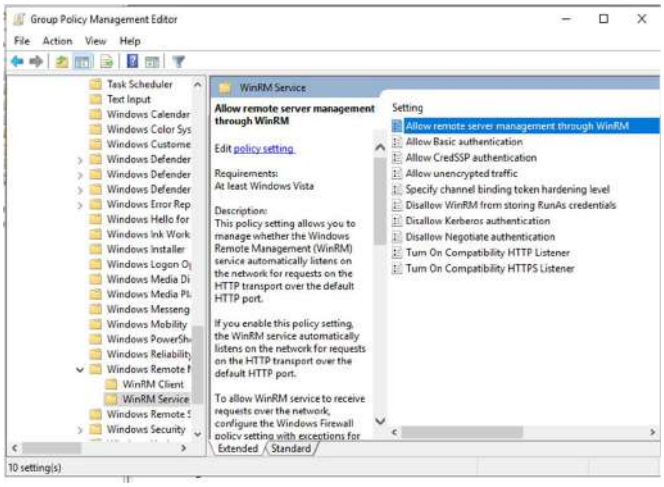
Right-click on “Enable WinRM Server” and choose **Edit**.



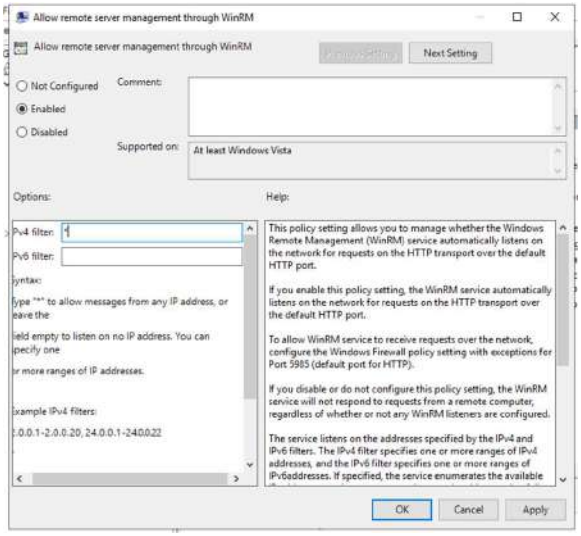
Using the sidebar go to the following folder: **Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Service**.



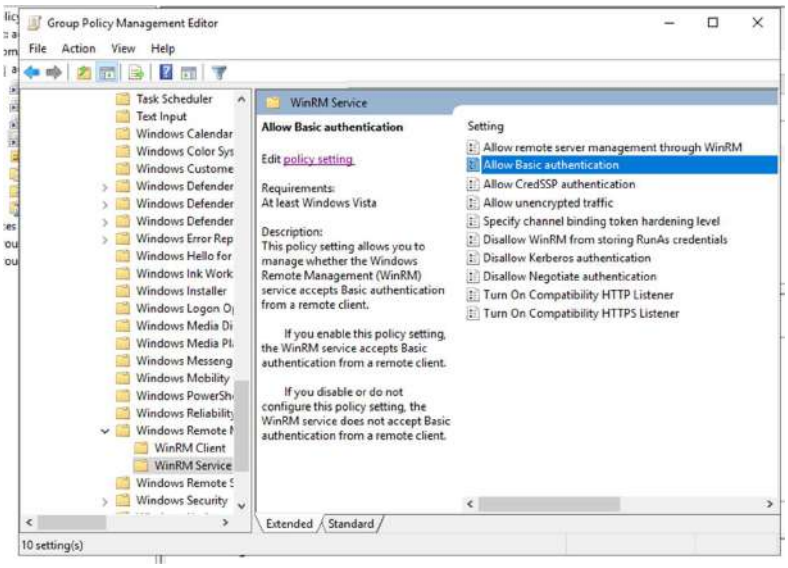
Select “Allow remote server management through WinRM” and then click on “Edit policy settings”.



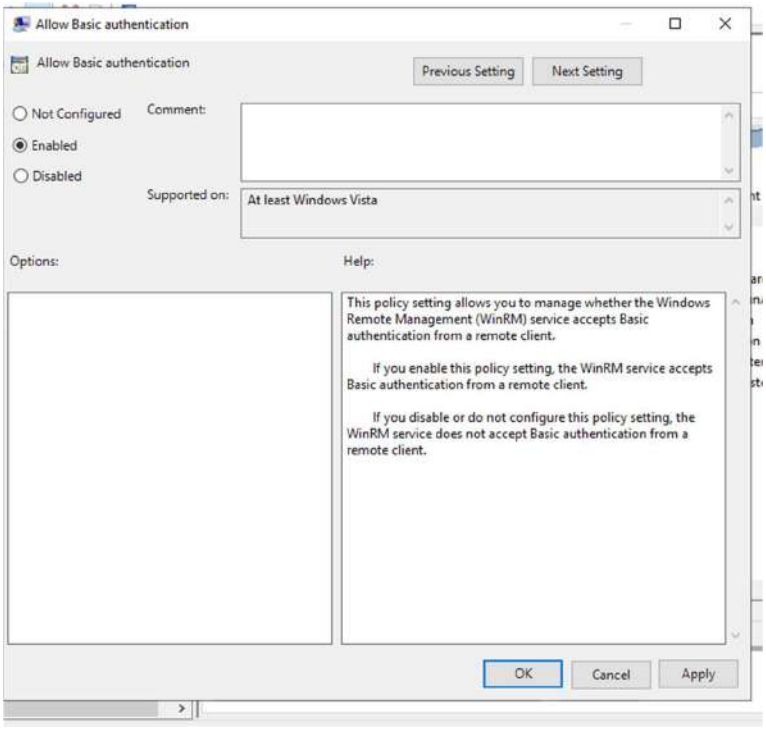
Set the policy to **Enabled**. In the Ipv4 filter field enter *****. Click on **Apply** then **OK**.



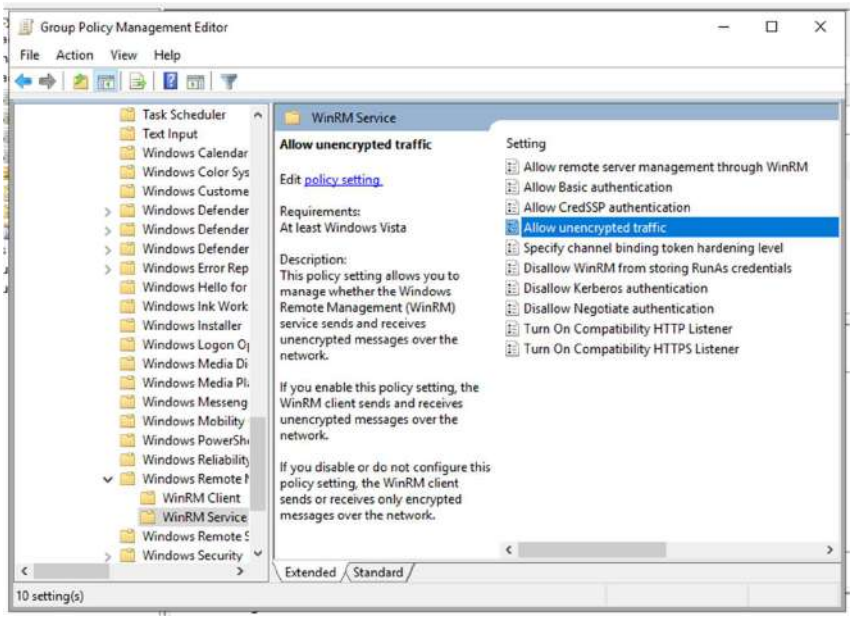
Select "Allow Basic authentication" and click on "Edit policy settings".



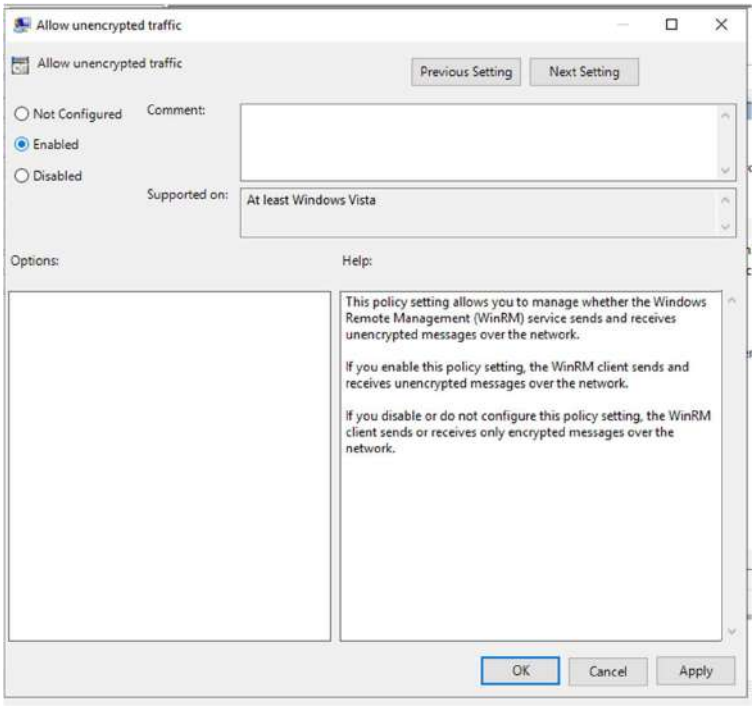
Set the policy to **Enabled**. Click on **Apply** and then **OK**.



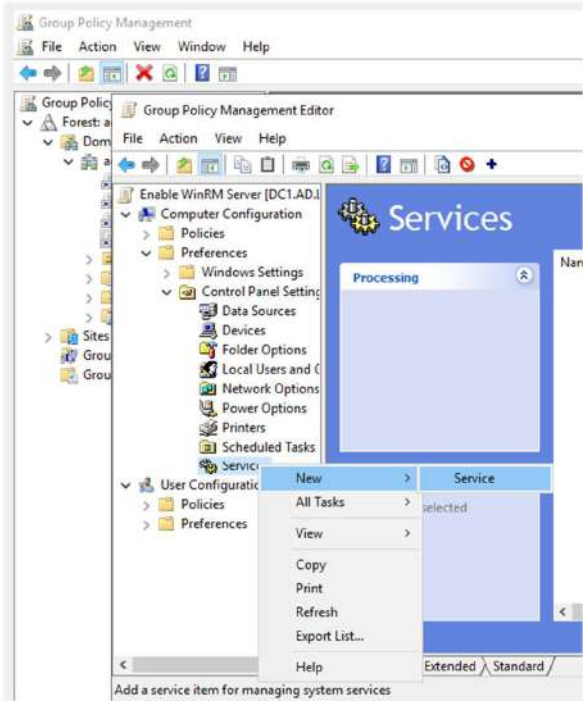
Select "Allow unencrypted traffic" and click on "Edit policy settings".



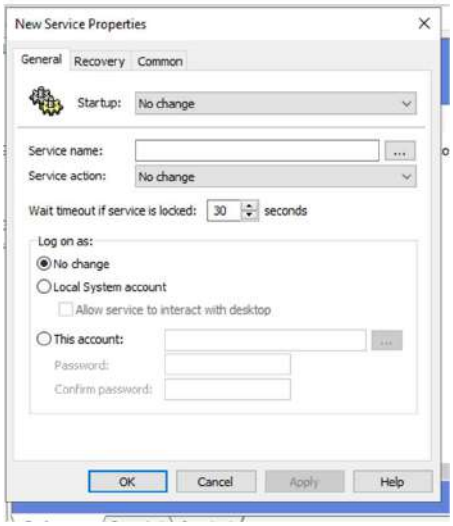
Set the policy to **Enabled**. Click on **Apply** then **OK**.



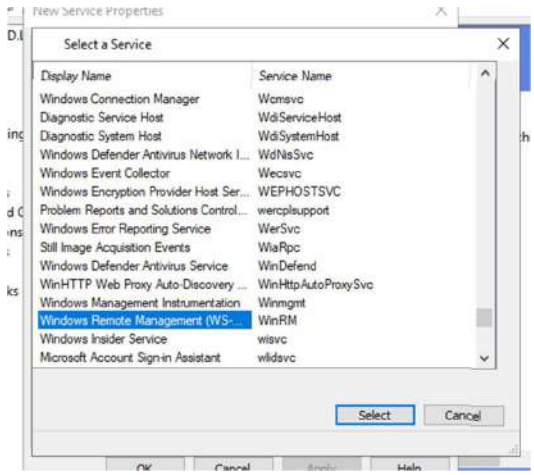
In the sidebar navigate to: **Computer Configuration -> Preferences -> Control Panel Settings**. Right-click on Services and select **New -> Service**.



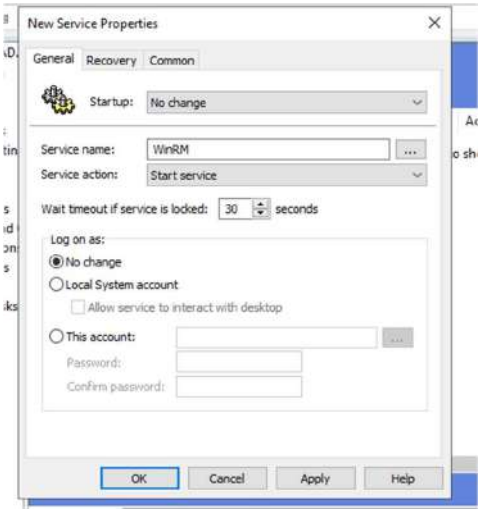
Select Startup to **Automatic**. Use the **…** button to select the Server name.



Select "Windows Remote Management (WS-Management)" and click on **Select**.

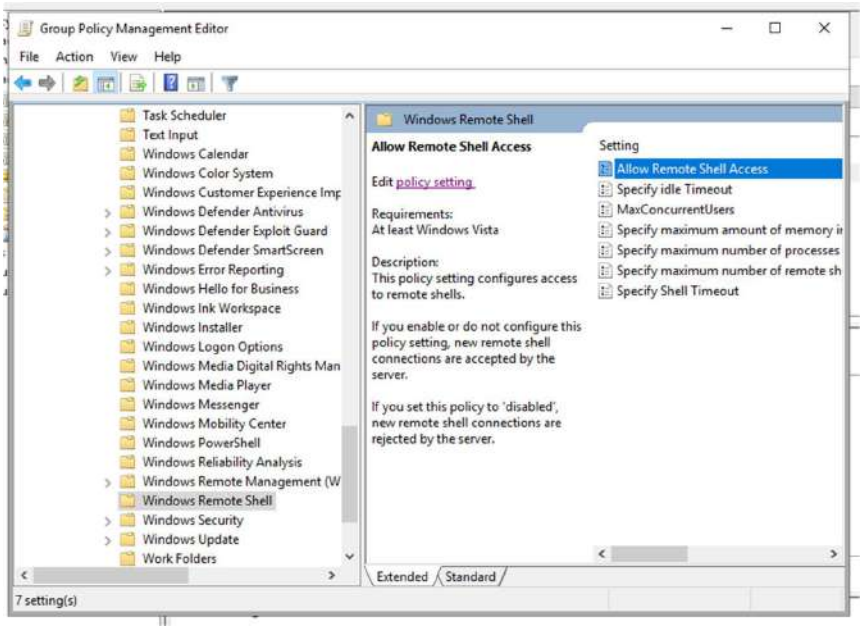


For Service action select **Start service**. Click on **Apply** then **OK**.

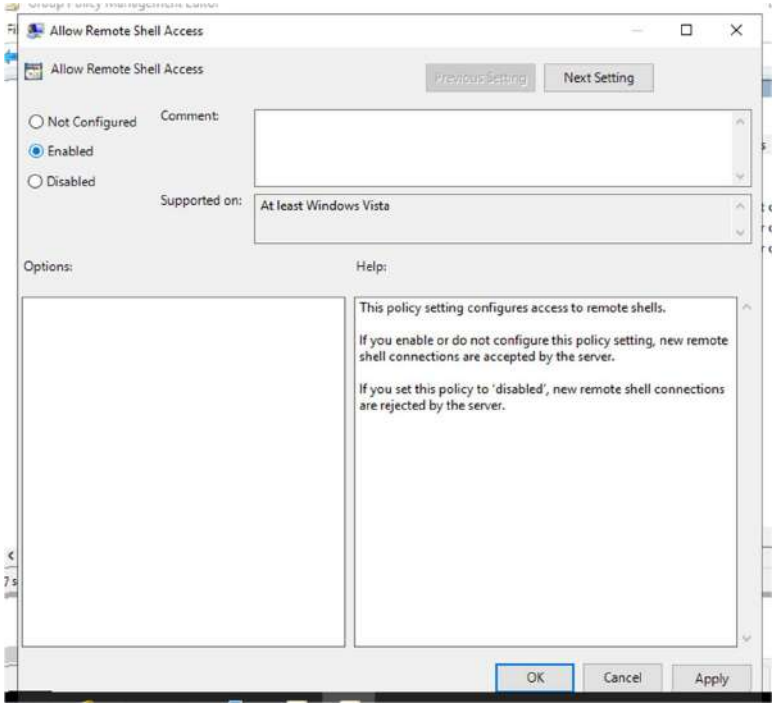


Using the sidebar navigate to the following location: **Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Remote Shell**

Select "Allow Remote Shell Access" and click on "Edit policy setting".

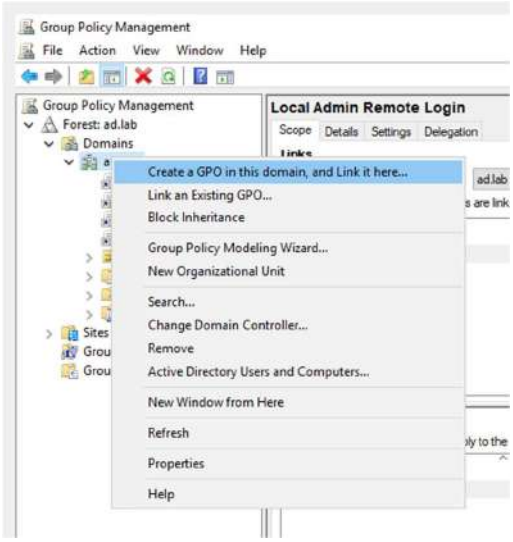


Set the policy to **Enabled**. Click on **Apply** then **OK**. Close the Group Policy Management Editor.

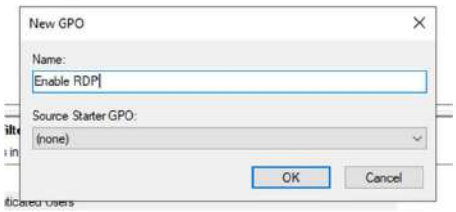


Enable RPC (Remote Procedure Call)

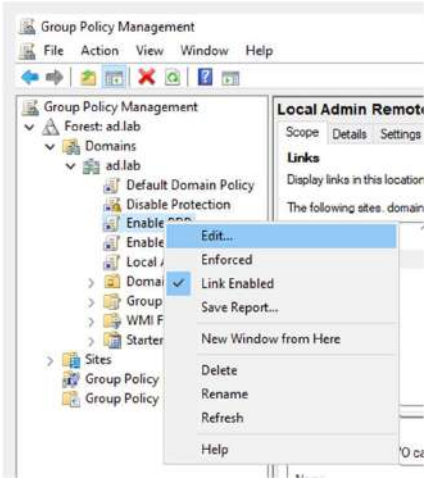
Right-click on the domain name. Select "Create a GPO in the domain and link here".



Give the GPO the name **Enable RPC**.

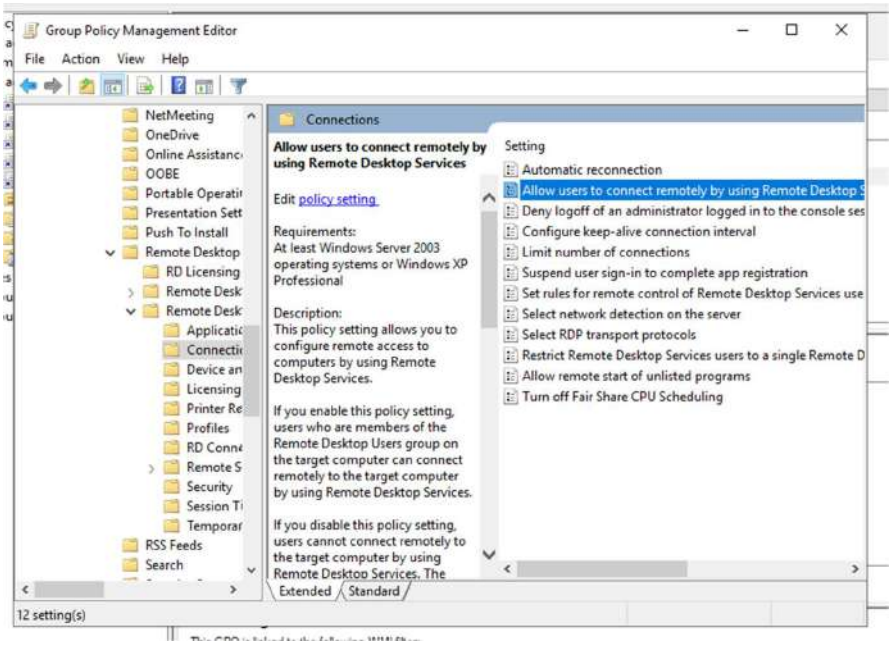


Right-click on "Enable RPC" and select **Edit**.

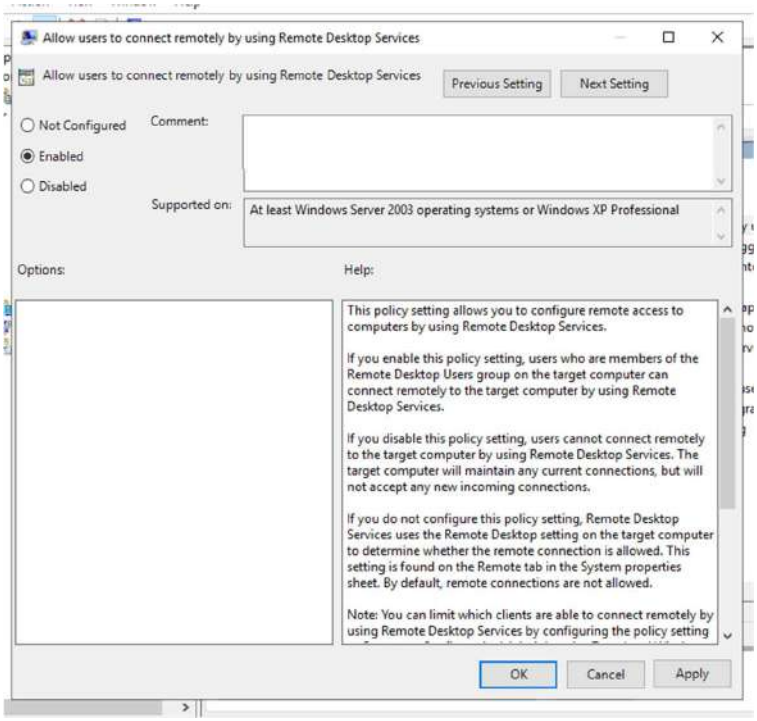


Using the sidebar navigate to the following folder: **Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Connections**.

Select "Allow users to connect remotely using Remote Desktop Services" and click on "Edit policy settings".

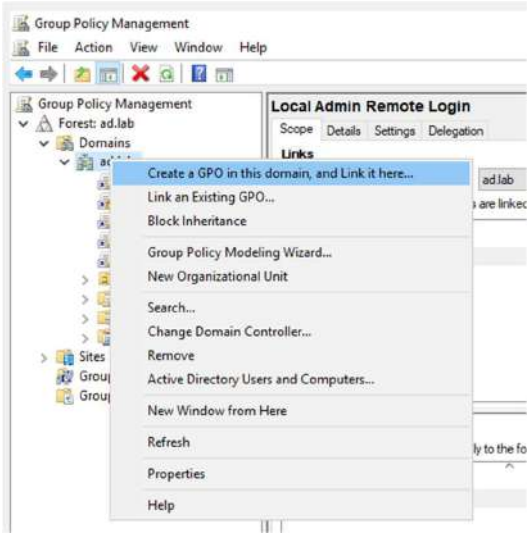


Set the policy to **Enabled**. Click on **Apply** then **OK**. Close Group Policy Management Editor.

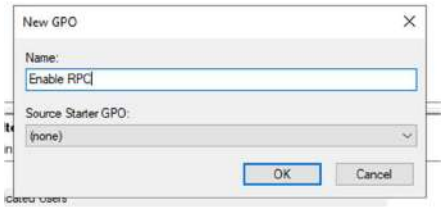


Enable RPC (Remote Procedure Call)

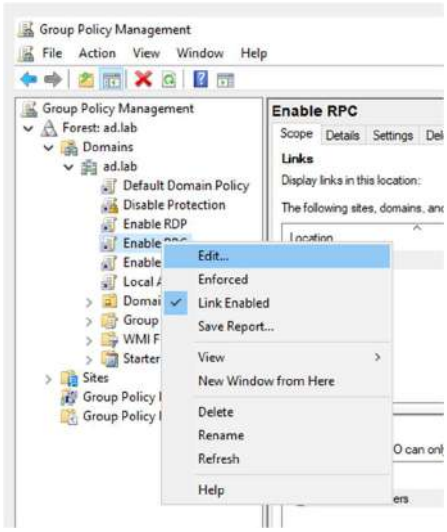
Right-click on the domain name. Select "Create a GPO in the domain and link here".



Give the GPO the name **Enable RPC**.

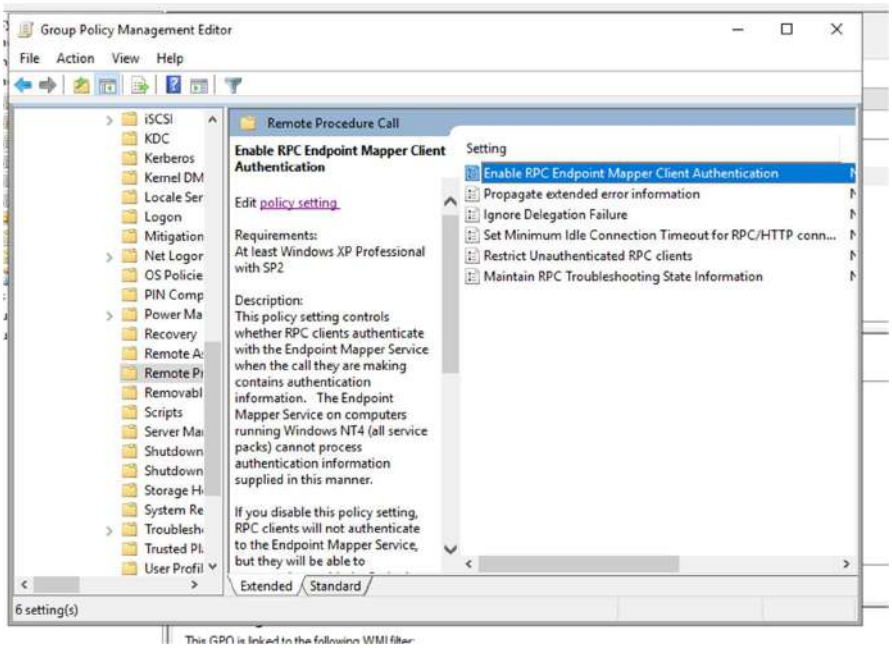


Right-click on "Enable RPC" and select **Edit**.

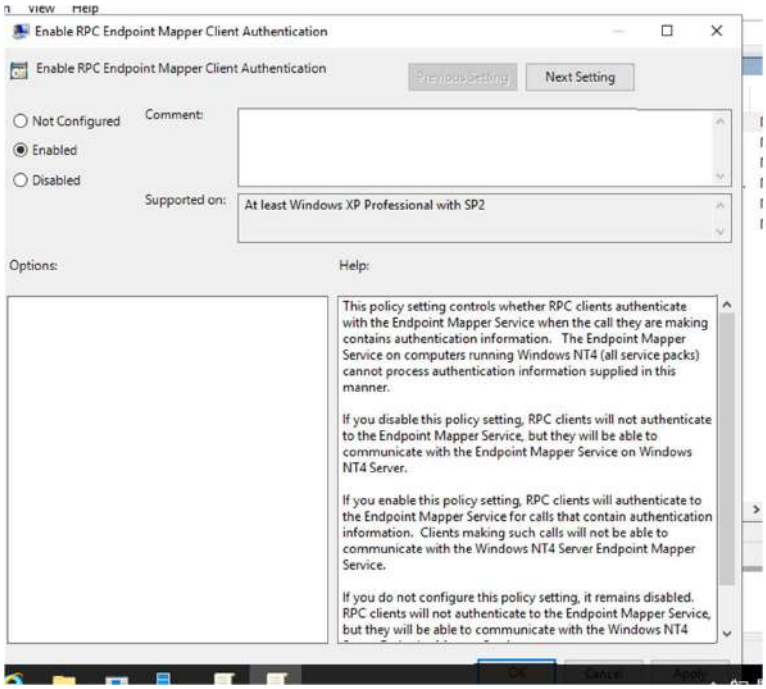


Using the sidebar navigate to the following folder: **Computer Configuration -> Administrative Templates -> System -> Remote Procedure Call**.

Select "Enable RPC Endpoint Mapper Client Authentication" and click on "Edit policy settings".

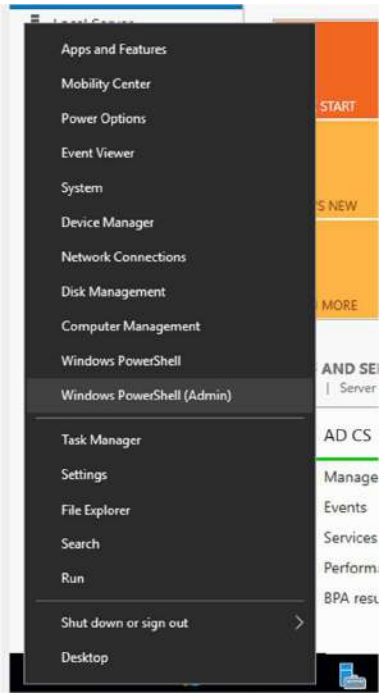


Set the policy to **Enabled**. Click on **Apply** then **OK**. Close Group Policy Management Editor.



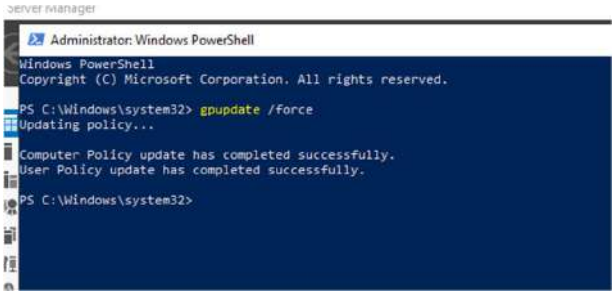
Enforce the Domain Policies

Right-click on the Start menu and select **Windows PowerShell (Admin)**.



In the terminal enter the following:

gpupdate /force



Now whenever a new device joins our AD environment the Group Policies that apply to all the devices will automatically be applied to them. With this, we have completed the Domain Controller setup.

Downloading Windows ISO File

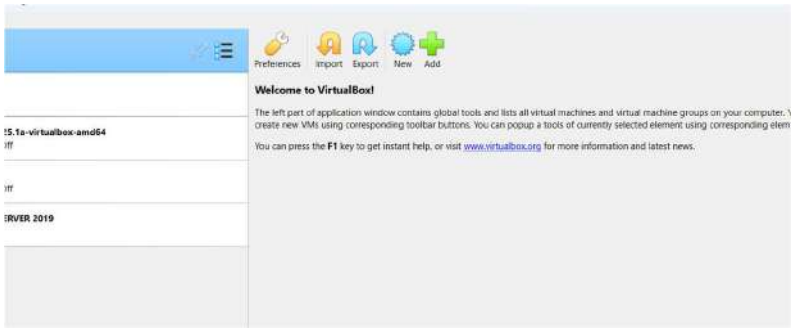
Windows 10 Enterprise

Go to the following URL: Windows 10 Enterprise | Microsoft Evaluation Center

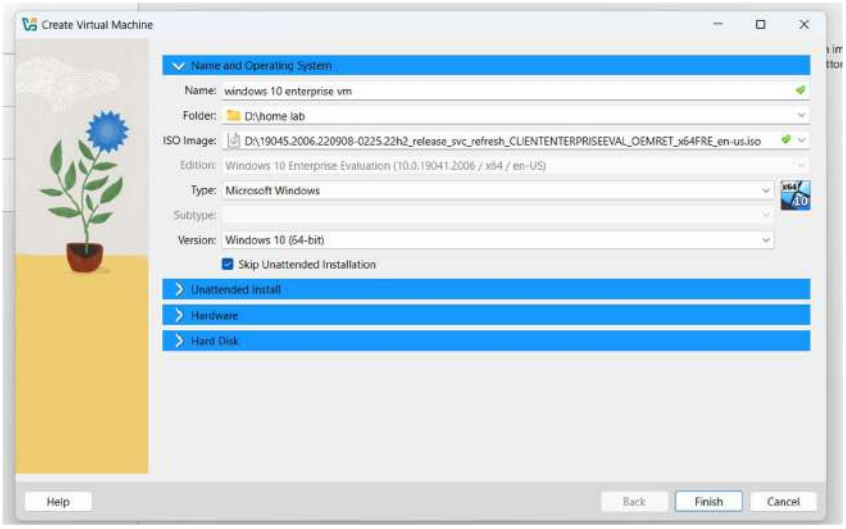
Click on the **64-bit edition** Enterprise ISO download option. The ISO file is ~5GB.

Windows 10 Enterprise VM

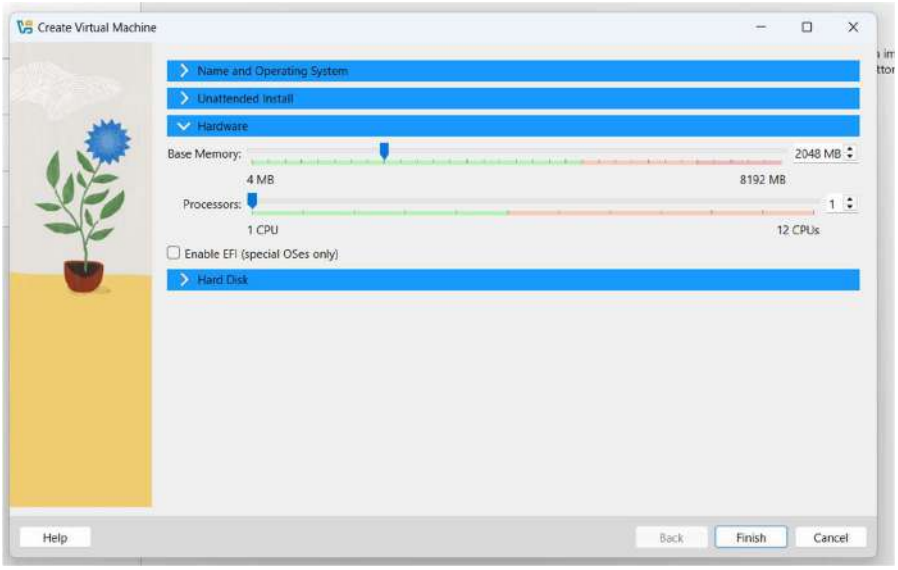
From the VirtualBox sidebar select Tools and then click on **New**.



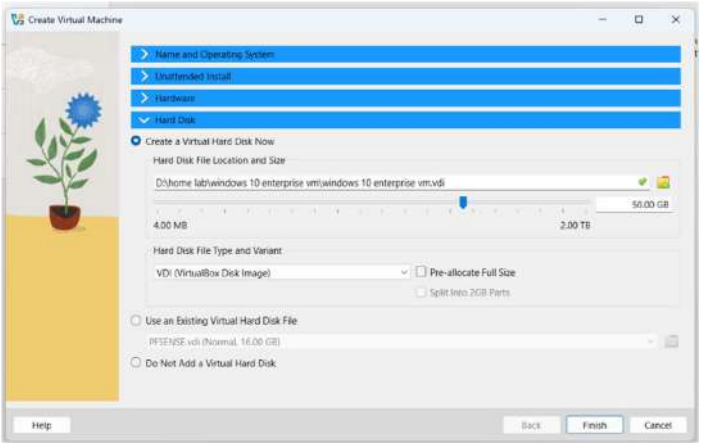
Give the VM a name. Ensure that the Folder option is pointing to the location where all the Home Lab VMs are saved. For the ISO Image option select the Windows 10 Enterprise image. Tick the **Skip Unattended Installation** option. Click on **Next** to continue.



Leave Memory and CPU on its default value. Click on **Next**.

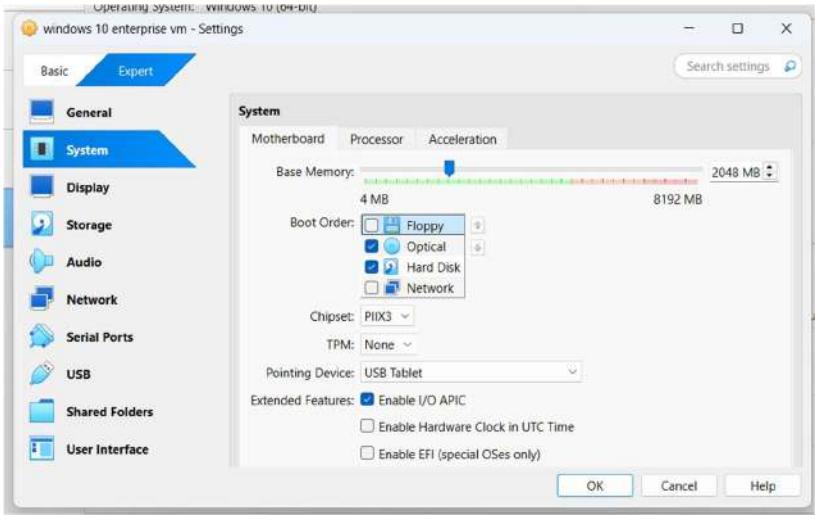


Increase the Hard Disk size to **50GB** and then click on **Finish**.

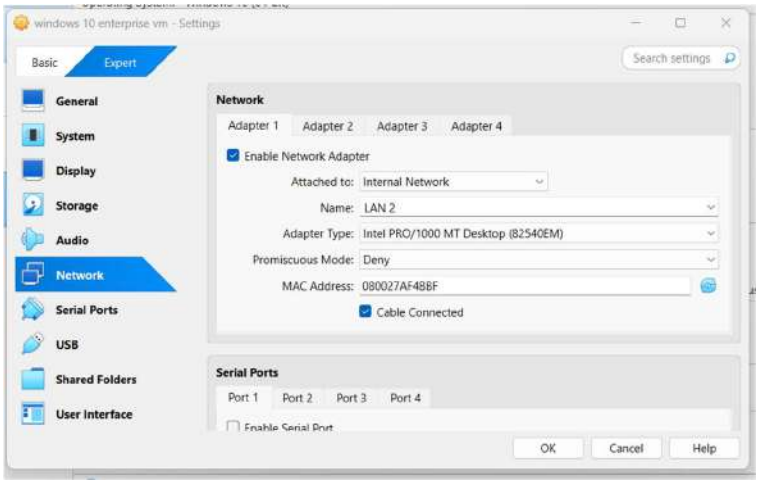


Select Windows 10 Enterprise VM from the sidebar and then from the toolbar choose **Settings**.

Go to **System -> Motherboard**. For Boot Order ensure **Hard Disk** is on the top followed by **Optical**. Disable **Floppy**.



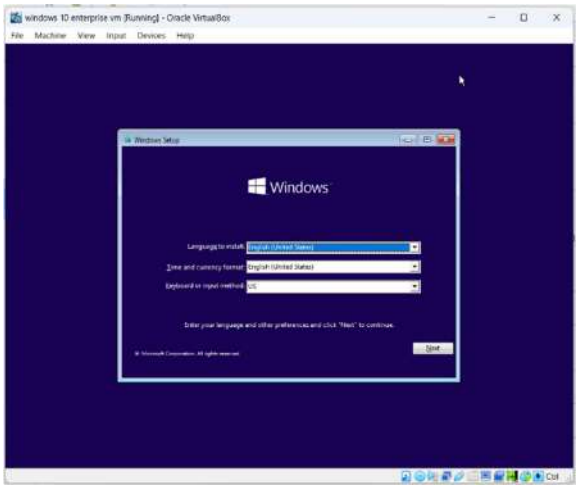
Go to **Network -> Adapter 1**. For the Attacked to field select **Internal Network**. For name select **LAN 2**. Click on **OK** to save the settings.



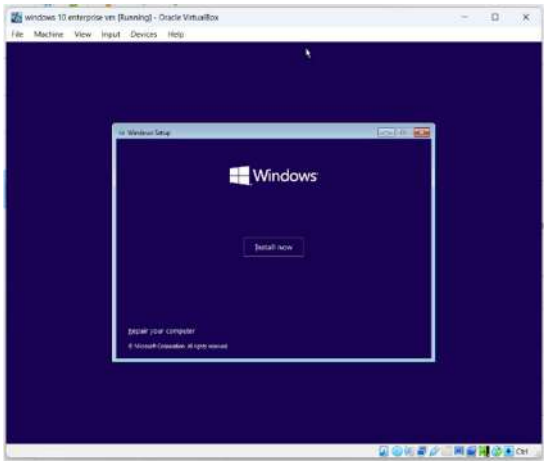
Select Windows 10 Enterprise VM from the sidebar then click on **Start**

OS Installation

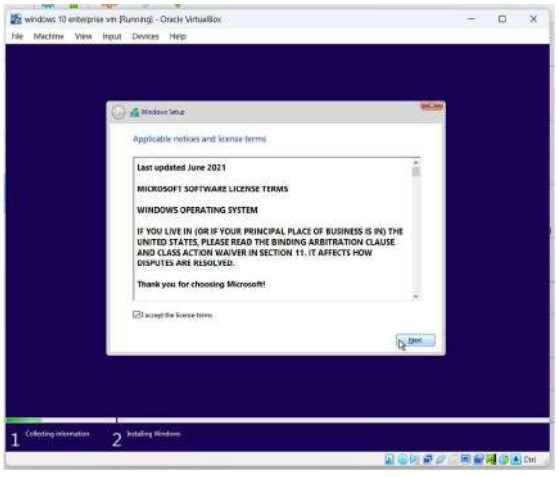
Click on **Next**.



Click on **Install now**.

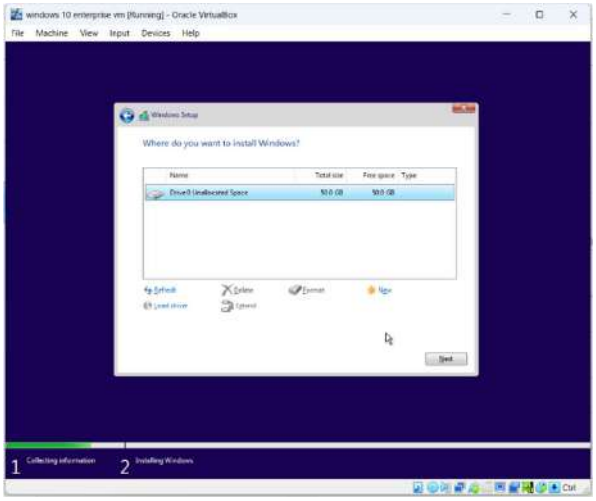


Accept the agreement and then click on **Next**.



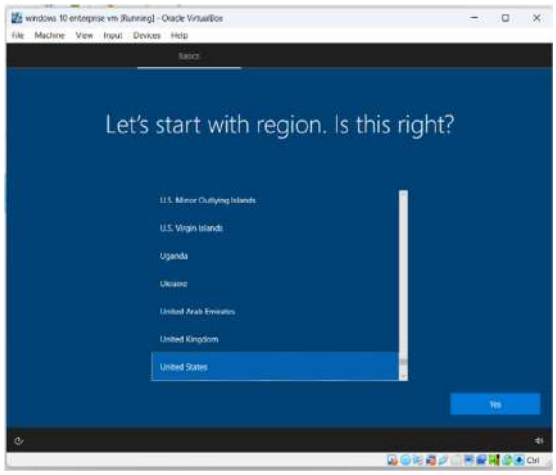
Select “Custom: Install Windows only (advanced)”.

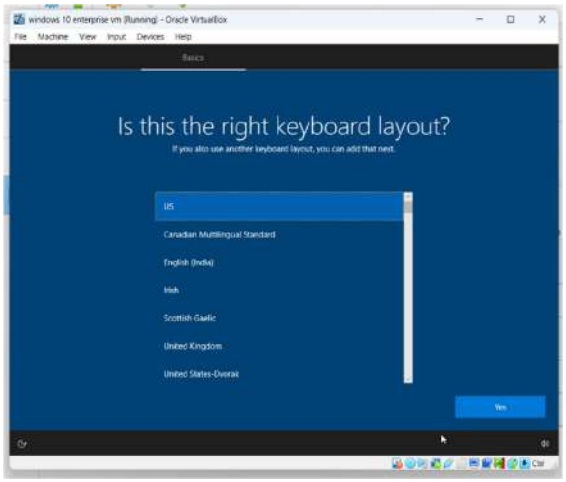
Then select **Disk 0** and then click on **Next**.



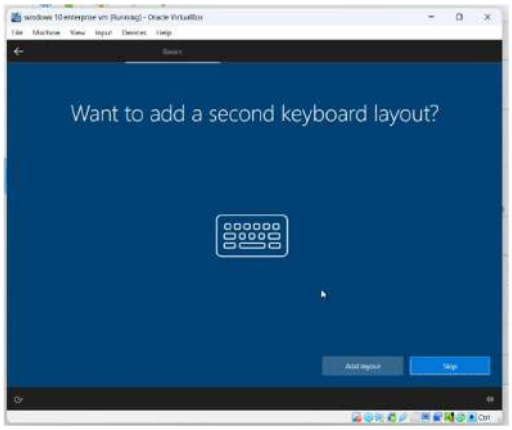
The VM will reboot multiple times during the installation.

Select your **Region** and **Keyboard Layout**.

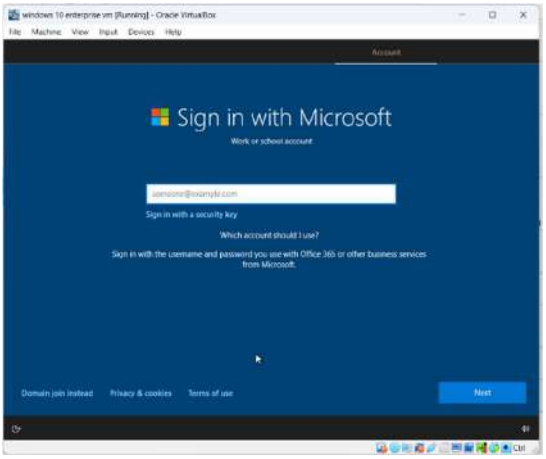




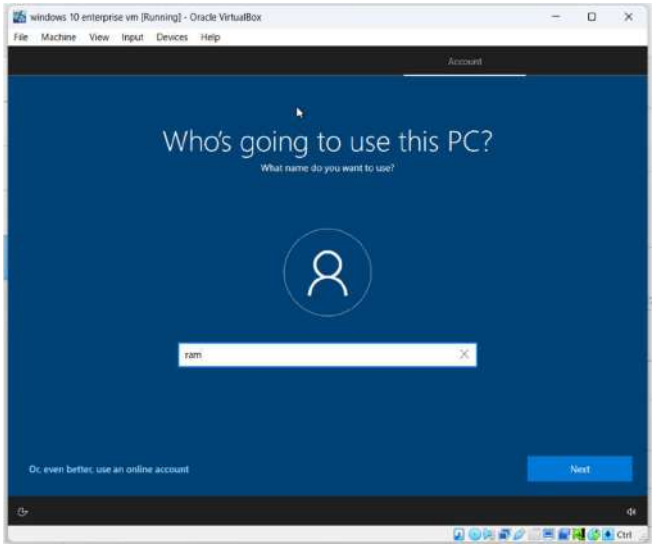
Click on **Skip**.



Select “Domain join instead”. This will allow us to configure a local account.

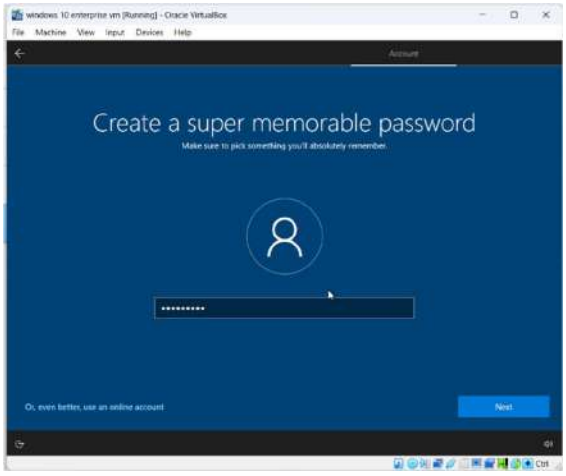


Enter a username and click on **Next**.

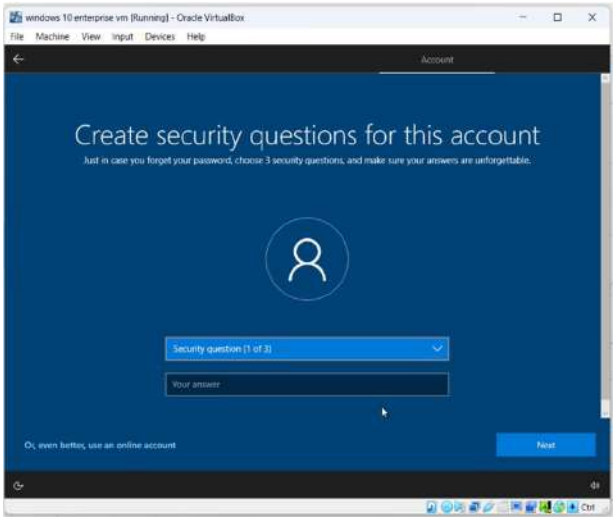


Enter a password and click on **Next**.

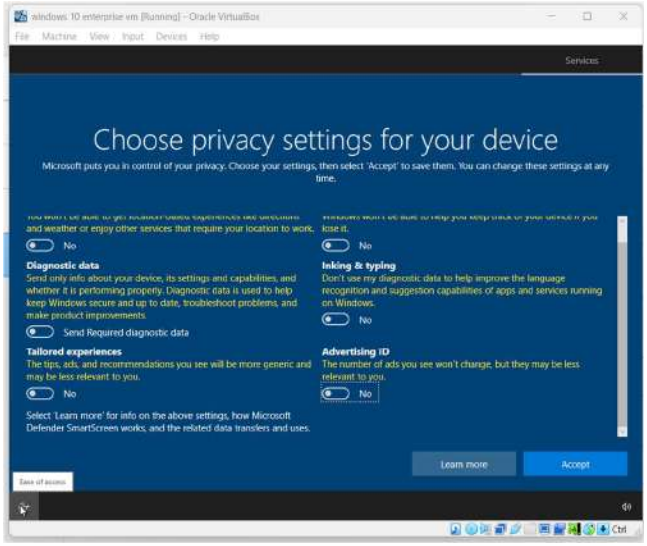
This password can be different from the password that was configured in Active Directory.



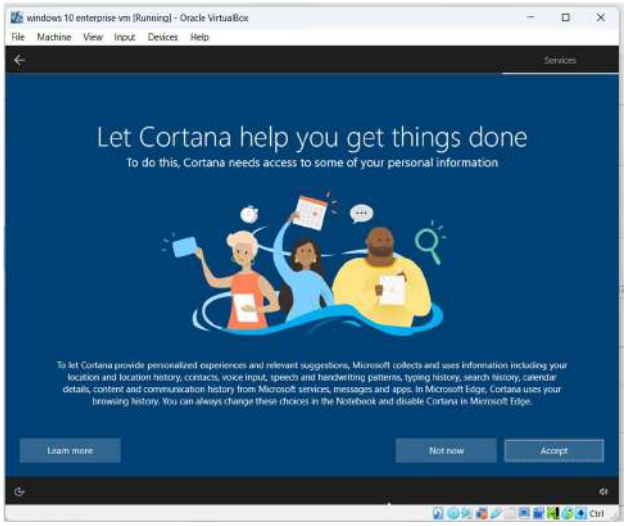
Configure the "Security Questions" for the user. Remember to note down these details in a secure location.



Disable all the features that are shown. Then click on **Accept**.



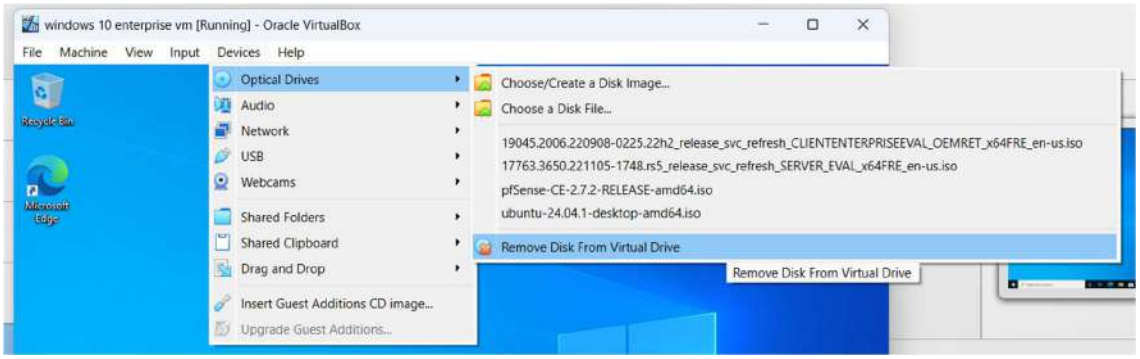
Select **Not now**.



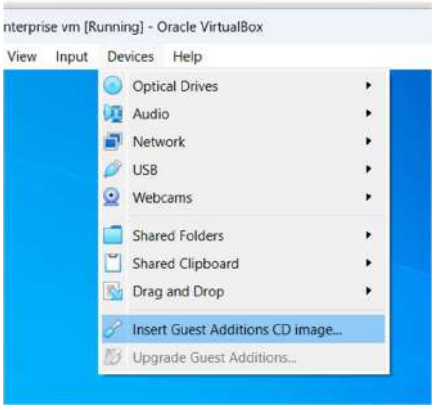
Once on the desktop a prompt to allow internet access should show up click on **Yes**.

Guest Additions Installation

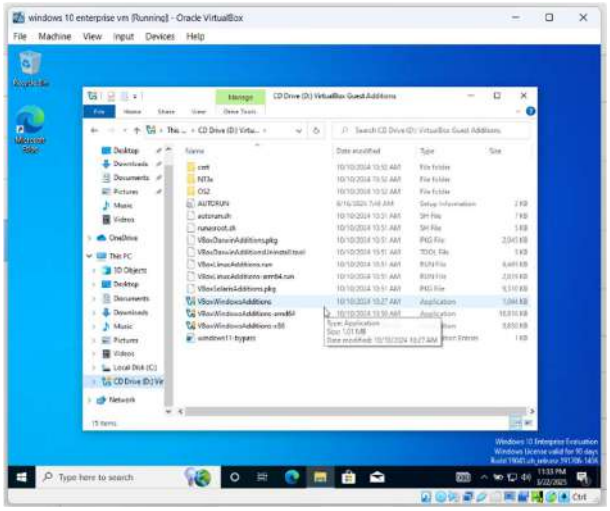
Similar to the Windows 2019 Server VM we need to install Guest Additions to enable Fullscreen mode. From the VM toolbar select **Devices -> Remove disk for virtual drive**. This will remove the Windows 10 image.



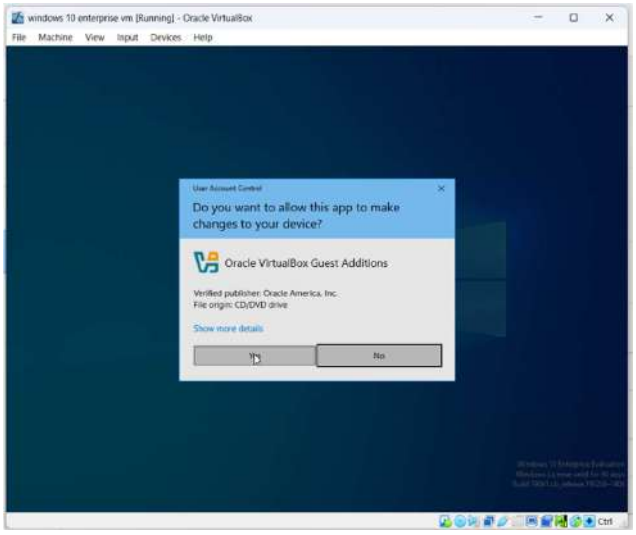
Click on **Devices -> Insert Guest Additions CD image**.



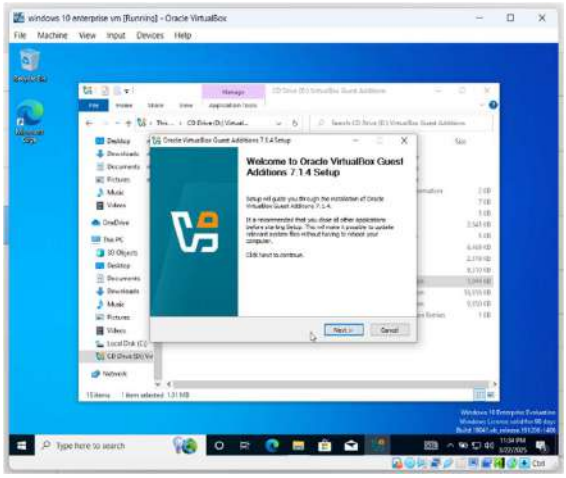
Open File Explorer. Once the disk has loaded from the sidebar select the disk drive. Double-click **VboxWindowsAdditions** to start the installer.



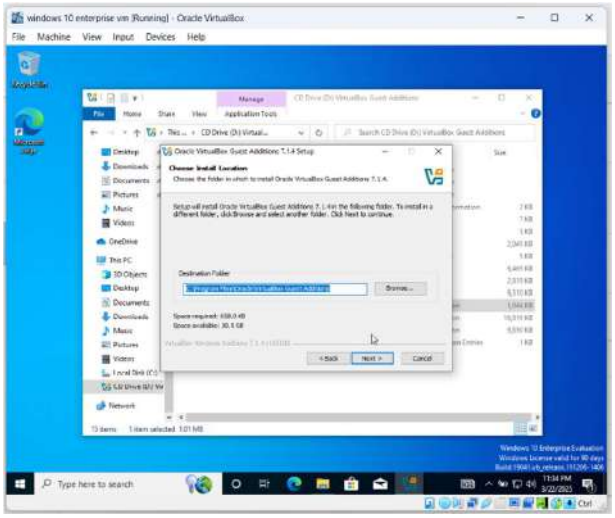
Click **Next**.



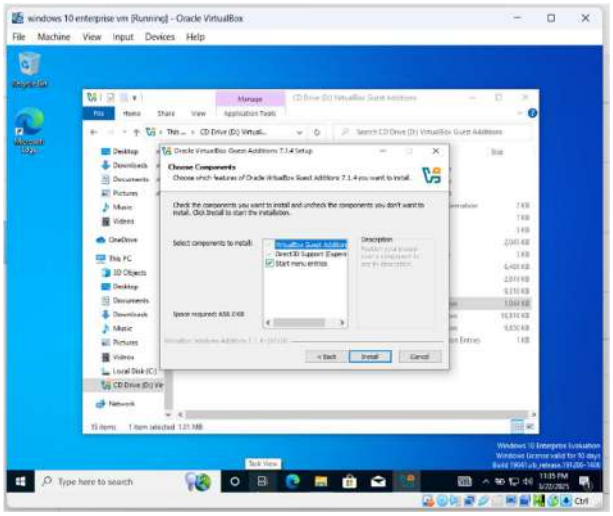
Click **Next**.



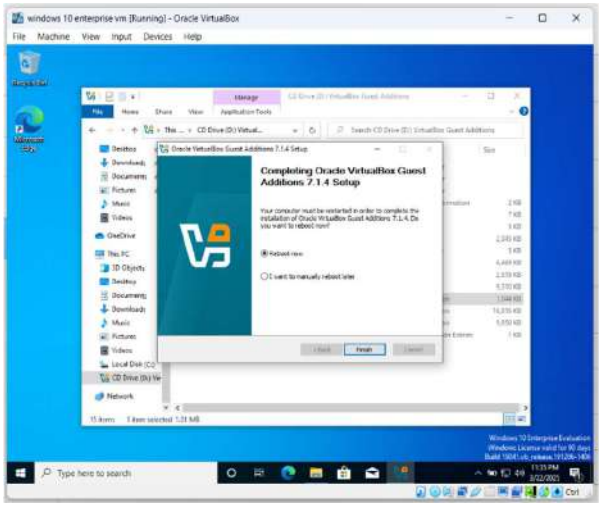
Click **Next**.



Click on **Install** to start the installation.

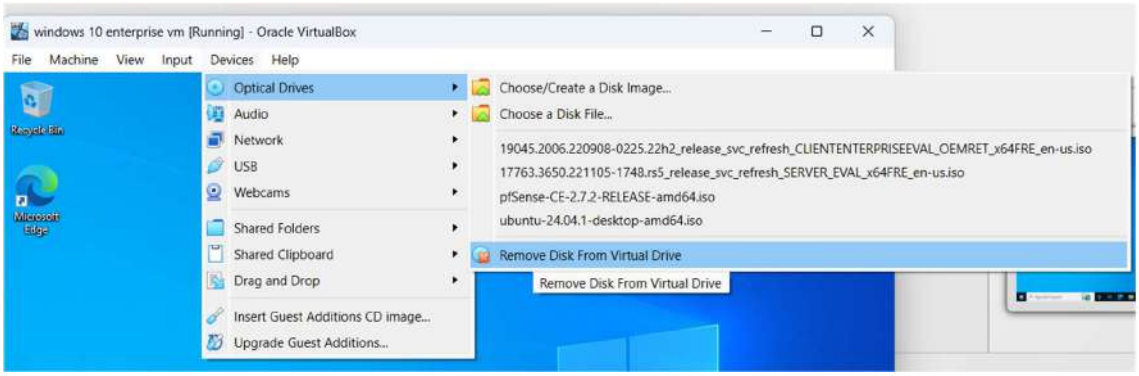


Select "Reboot now" and then click on **Finish**. The VM will reboot.



Login into the system.

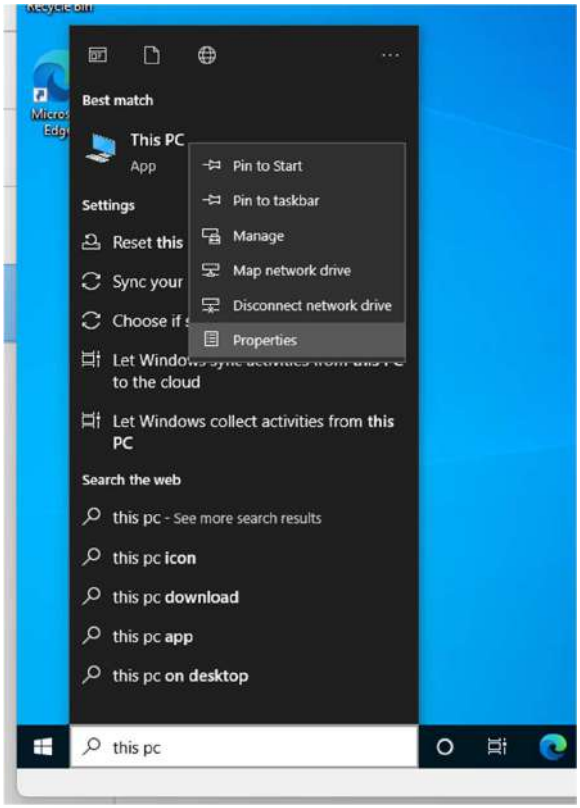
From the toolbar select **Optical Devices -> Remove disk from virtual drive** to remove the Guest Additions image.



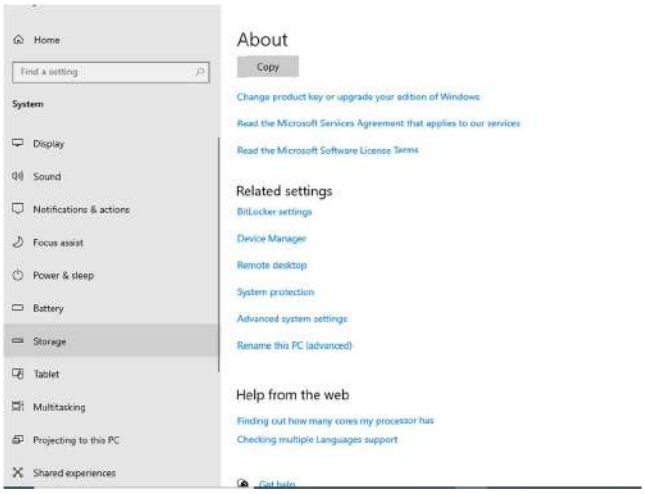
Use the shortcut **Ctrl+F** to enter Fullscreen mode. Use the same key to exit Fullscreen. The VM should automatically scale to fit the window size.

Now we can add this device to the AD domain and log in as an AD user.

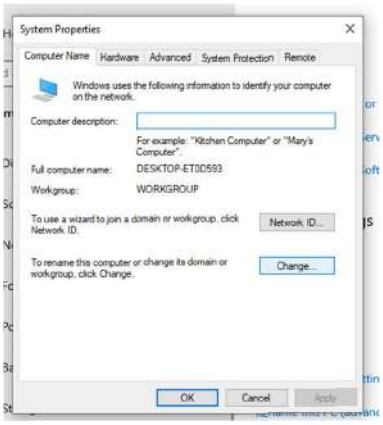
Click on the Search Bar and search for "This PC". Right-click on it and select **Properties**.



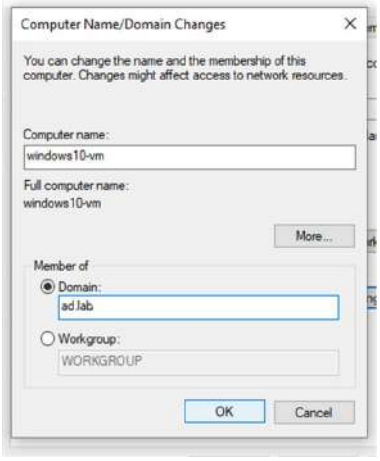
Click on **Advanced system settings**.



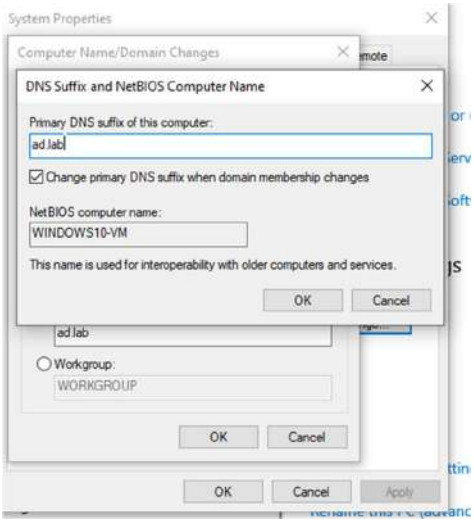
Select the "Computer Name" tab and click on **Change**.



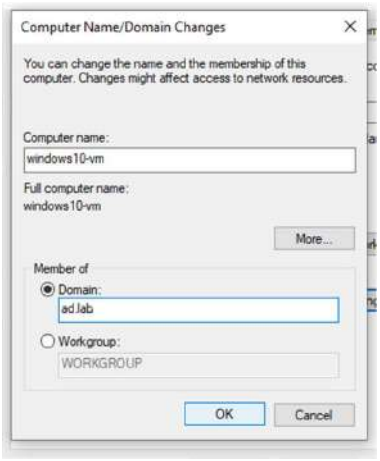
In the Computer name field enter a name that can be used to easily identify this VM. In the Member of section select **Domain** and enter the name of the AD domain (in my case **ad.lab**). Then click on **More**.



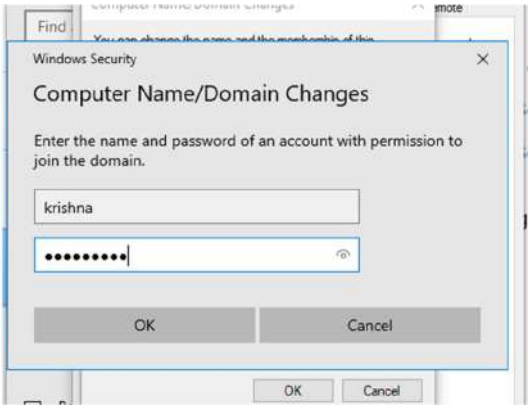
In the "Primary DNS suffix of this computer" field enter the domain name. Click on **OK**.



Click on **OK**.

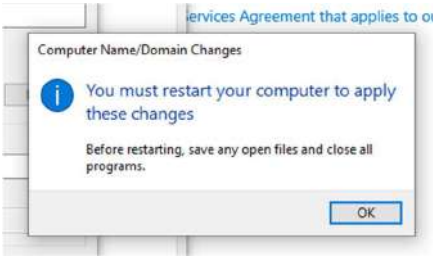


Now a popup should appear. Enter the login name and password of the Domain Admin and click on **OK**.



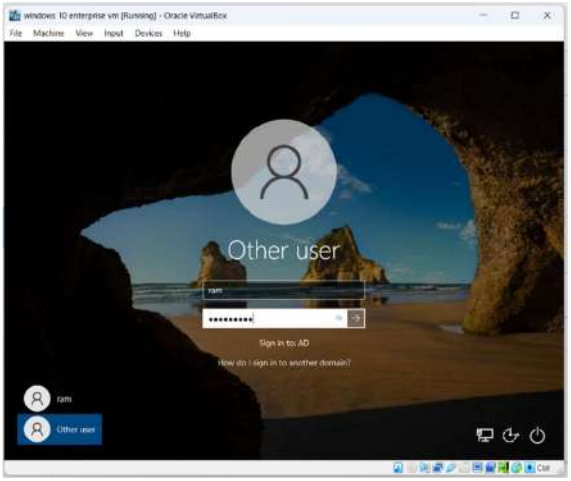
The device will be added to the AD environment. Click on **OK**.

The device needs to be rebooted to apply the domain-specific settings. Click on **OK** to continue.

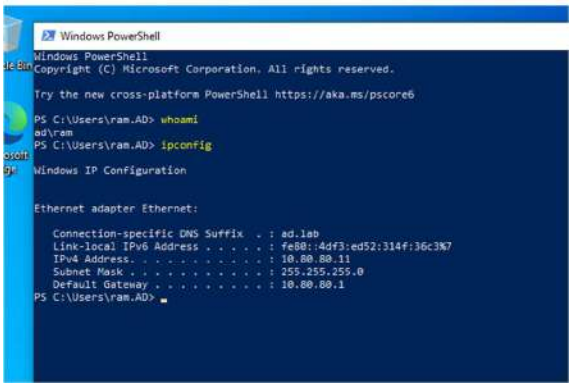


Click on "Restart Now".

Once on the login screen. Click on "Other user". Enter the login name and password of the AD user that will use this device and press **Enter**.



Now we are logged into the system as the AD user. To confirm this we can open PowerShell and run **whoami**.



MALWARE ANALYSIS

VirtualBox GUI does not allow us to create more than four Network Interfaces.

However, we can configure up to 8 interfaces per VM. To add more than 4 interfaces we have to utilize the VirtualBox CLI.

To be able to use the CLI we have to add its path as an environment variable.
VirtualBox is by default installed at **C:\Program Files\Oracle\VirtualBox**.

Copy the path to the executable from the navigation bar.

Open Search and type "Environment". Click on **Edit environment variables for your account**.

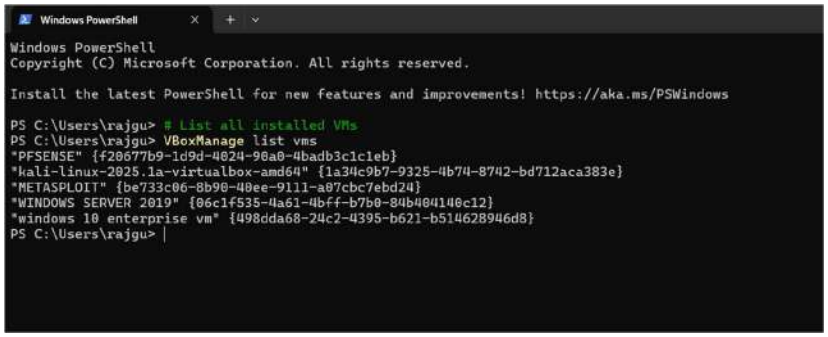
In the top window select the variable named "Path" and then click on **Edit**.

Click on **New** and then paste the path to the VirtualBox CLI. Then click on **OK**.

Click on OK to close the Environment Variables menu.

To test if the variable was added successfully open PowerShell and run the following command:

List all installed VMs:-> **VBoxManage list vms**



Before we create the new interfaces we need to know the name of the pfSense VM (it is "pfSense" in my case). The VM should also be "Powered Off".

To add a network interface run the following commands:

Create a Internet Network : **VBoxManage modifyvm "PFSENSE" --nic5 intnet**

Use the Paravirtualized Adapter : **VBoxManage modifyvm "PFSENSE" --nictype5 virtio**

Give it the name LAN 3 : **VBoxManage modifyvm "PFSENSE" --intnet5 "LAN 3"**

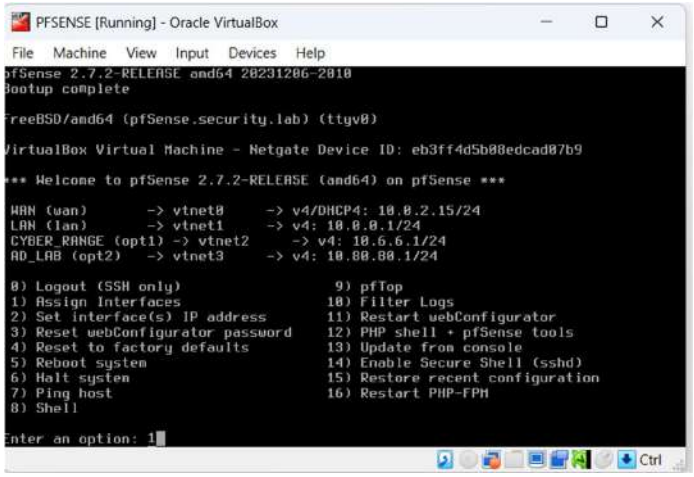
Network Int connected by Cable: **VBoxManage modifyvm "PFSENSE" --cableconnected5 on**

```
PS C:\Users\rajgu> VBoxManage modifyvm "PFSENSE" --nic5 intnet
PS C:\Users\rajgu> VBoxManage modifyvm "PFSENSE" --nictype5 virtio
PS C:\Users\rajgu> VBoxManage modifyvm "pPFSENSE" --intnet5 "LAN 3"
VBoxManage.exe: error: Could not find a registered machine named 'pPFSENSE'
VBoxManage.exe: error: Details: code VBOX_E_OBJECT_NOT_FOUND (0x80bb0001), component VirtualBoxWrap, interface IVirtualB
ox, callee IUnknown
VBoxManage.exe: error: Context: "FindMachine(Bstr(a->argv[0]).raw(), machine.asOutParam())" at line 841 of file VBoxMana
geModifyVM.cpp
PS C:\Users\rajgu> VBoxManage modifyvm "PFSENSE" --intnet5 "LAN 3"
PS C:\Users\rajgu> VBoxManage modifyvm "PFSENSE" --cableconnected5 on
PS C:\Users\rajgu>
```

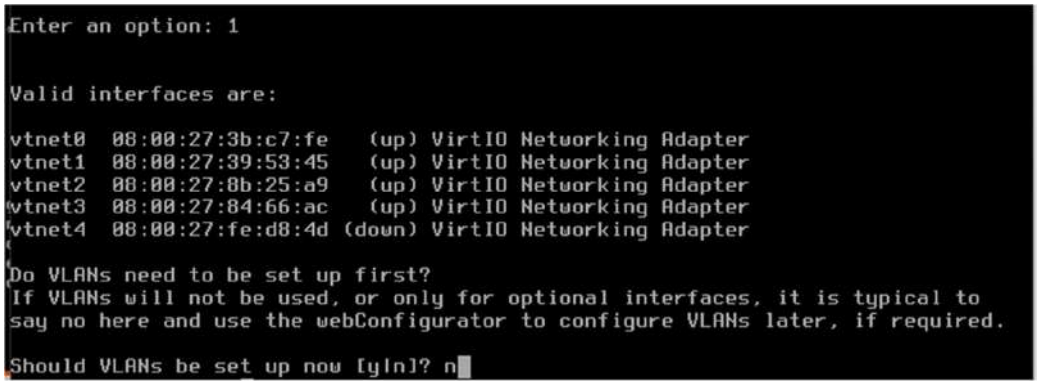
Now if we look at the overview of the pfSense VM we should see Adapter 5.

Enabling the Interface

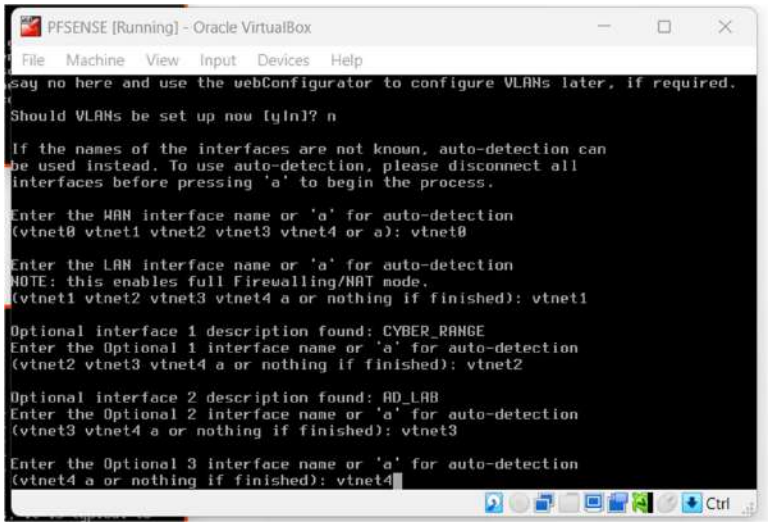
Start the pfSense VM. On boot, you will notice that there are still only 4 interfaces. The new interface has to be onboarded before it shows up in pfSense.



Enter **1** to select “Assign Interfaces”.
Should VLANs be set up now? **n**

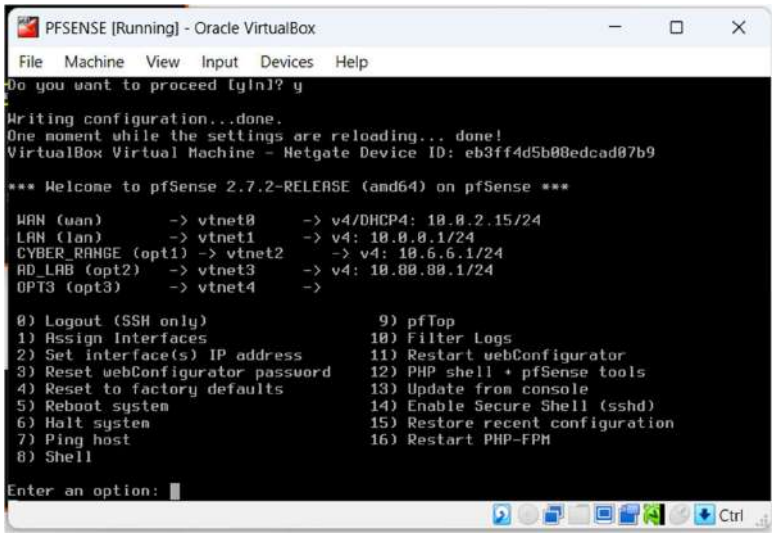


Enter the WAN interface name: **vtnet0**
Enter the LAN interface name: **vtnet1**
Enter the Optional 1 interface name: **vtnet2**
Enter the Optional 2 interface name: **vtnet3**
Enter the Optional 3 interface name: **vtnet4**

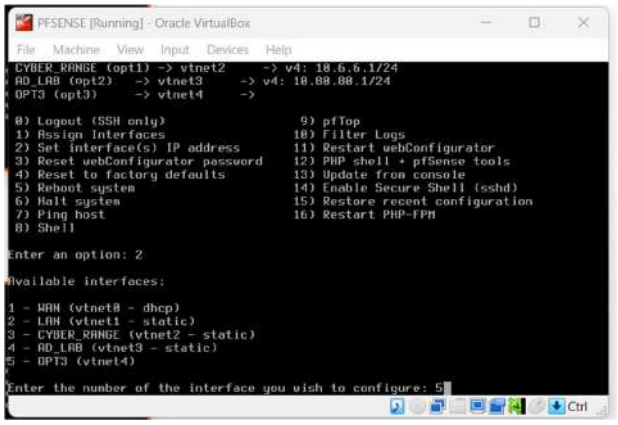


Do you want to proceed?: **y**

The new interface has been added. Now we need to assign the interface an IP address.



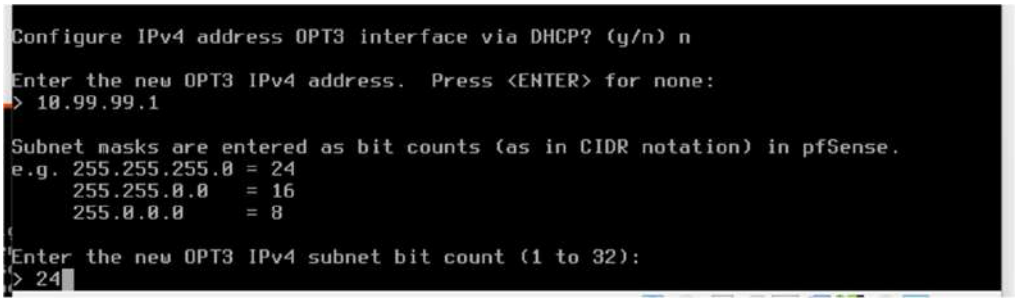
Enter **2** to select “Set interface(s) IP address”
Enter **5** to select the OPT3 interface.



Configure IPv4 address OPT3 interface via DHCP?: **n**
Enter the new OPT3 IPv4 address: **10.99.99.1**
Enter the new OPT3 IPv4 subnet bit count: **24**

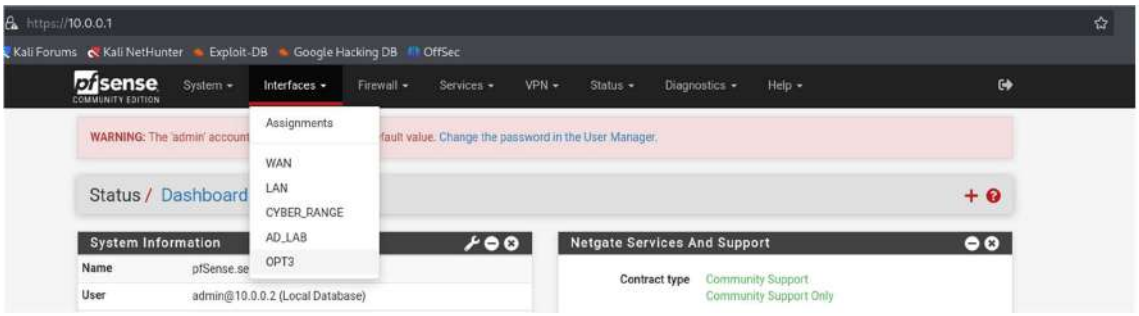
For the next question press **Enter**. Since we are configuring a LAN interface we do not have to worry about the upstream gateway.

Configure IPv6 address OPT3 interface via DHCP6: **n**
For the new OPT3 IPv6 address question press **Enter**.
Do you want to enable the DHCP server on OPT3?: **y**
Enter the start address of the IPv4 client address range: **10.99.99.11**
Enter the end address of the IPv4 client address range: **10.99.99.243**
Do you want to revert to HTTP as the webConfigurator protocol?: **n**

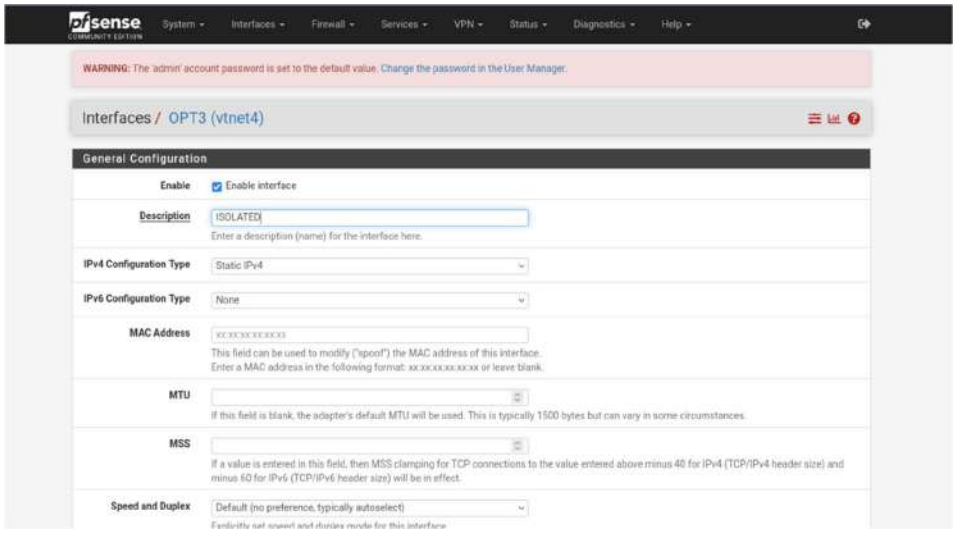


Now interface OPT3 will have an IP address.

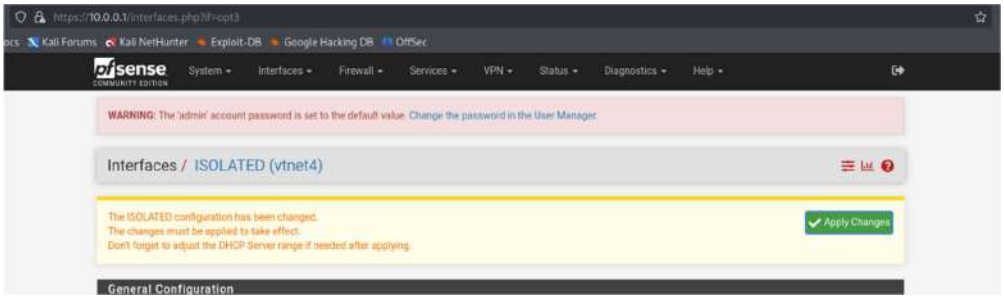
Launch the Kali Linux VM. Login to the pfSense web portal. From the navigation bar select **Interfaces -> OPT3**.



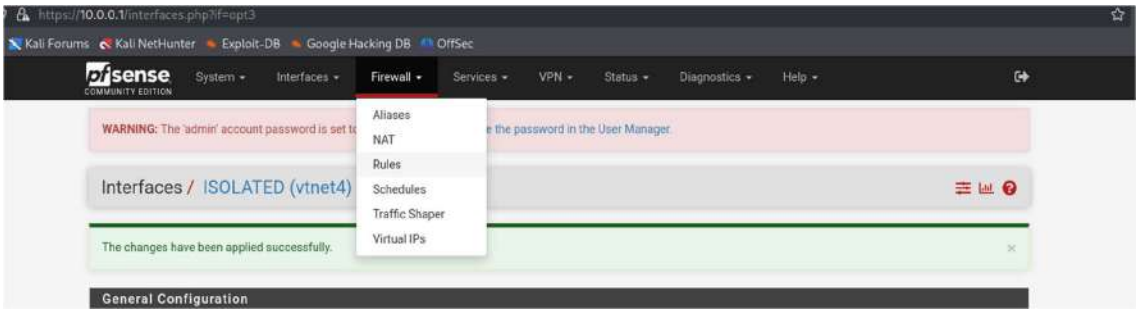
In the description field enter **ISOLATED**. Scroll to the bottom and click on **Save**.



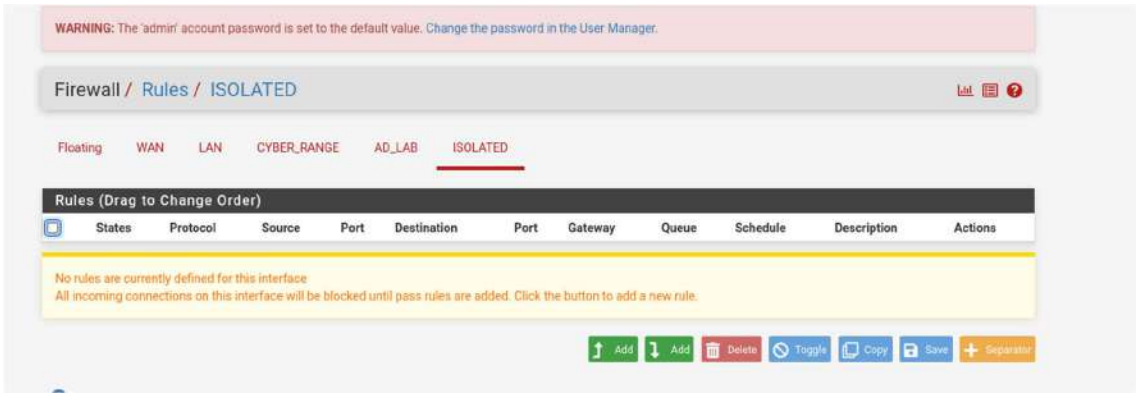
Click on **Apply Changes** in the popup that appears to persist the changes.



From the navigation bar click on **Firewall -> Rules**.

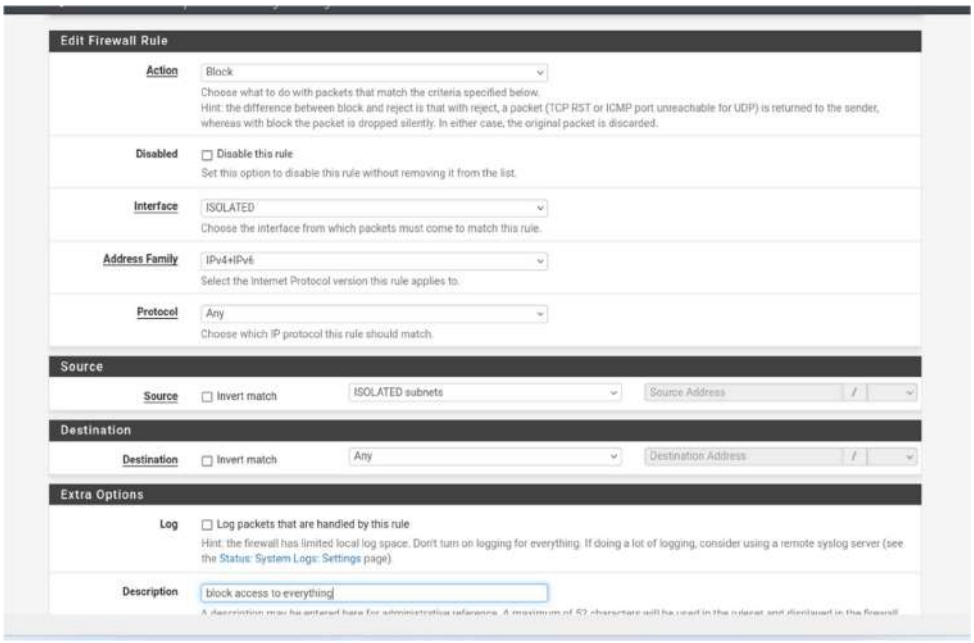


Select the **ISOLATED** tab. Click on the "Add" button to create a new rule.

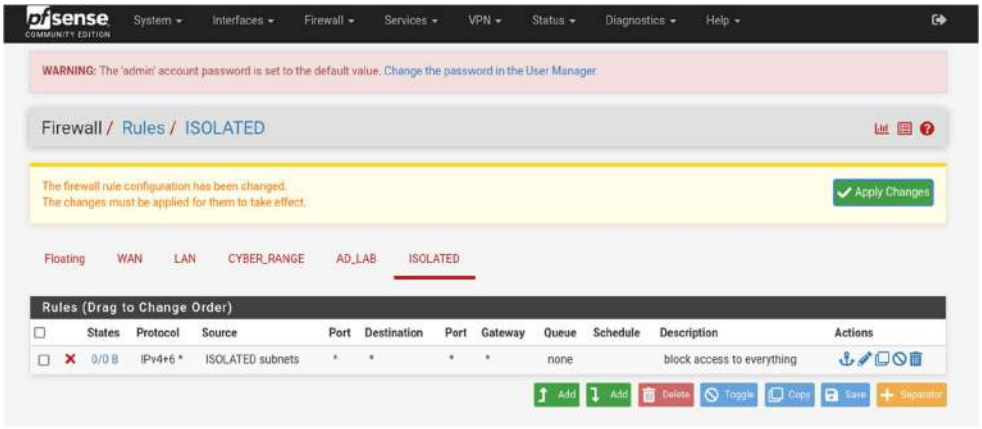


Change the values as follows:
Action: **Block**
Address Family: **IPv4+IPv6**
Protocol: **Any**
Source: **ISOLATED subnets**
Description: **Block access to everything**

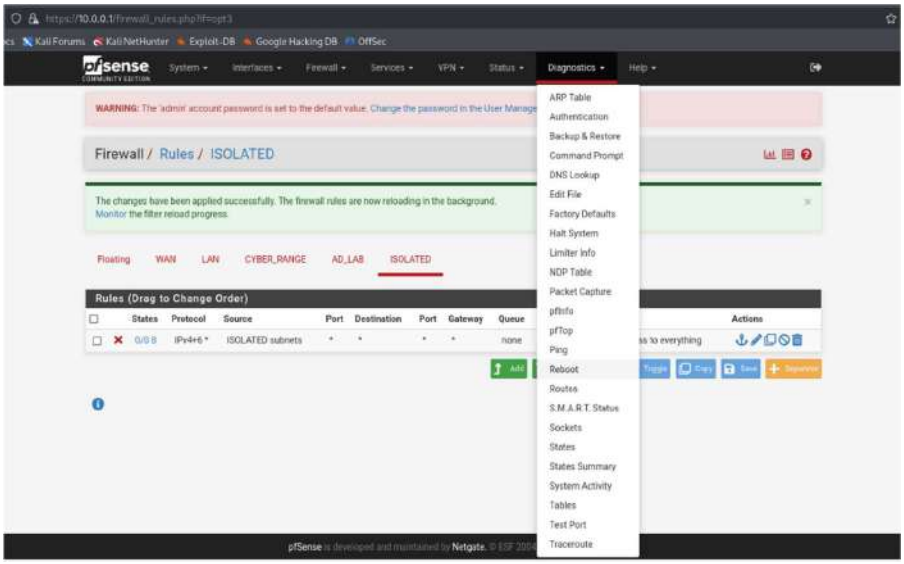
Scroll to the bottom and click on **Save**.



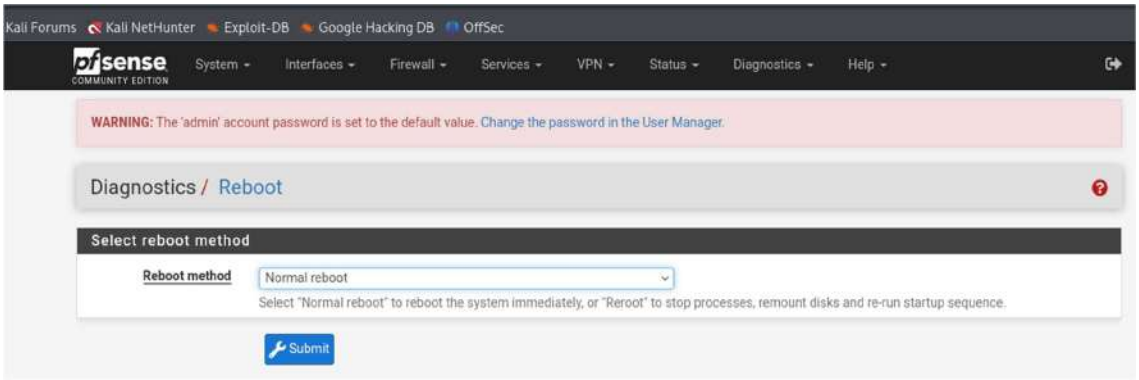
In the popup click on **Apply Changes** to persist the new rule.



Now we need to restart pfSense to ensure that the firewall rules are propagated properly. From the navigation bar select **Diagnostics -> Reboot**.



Click on **Submit**.



Once pfSense boots up you will be redirected to the login page.

Windows ISO Download

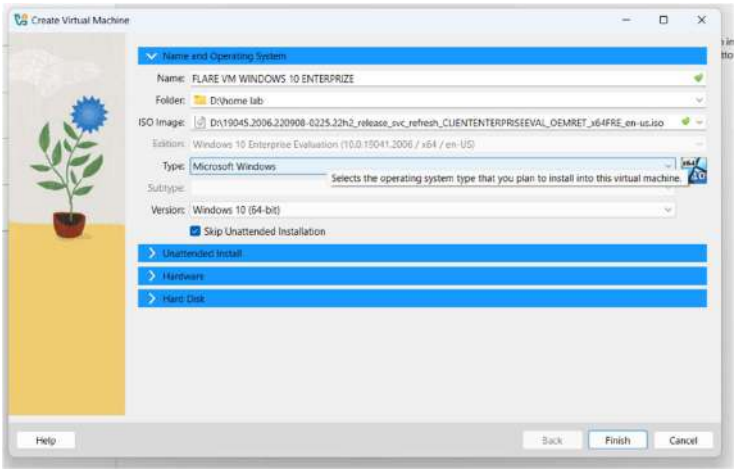
Go to the following URL: Windows 10 Enterprise | Microsoft Evaluation Center

Click on the 64-bit edition Enterprise ISO download option. The ISO file is ~5GB.

Creating the VM

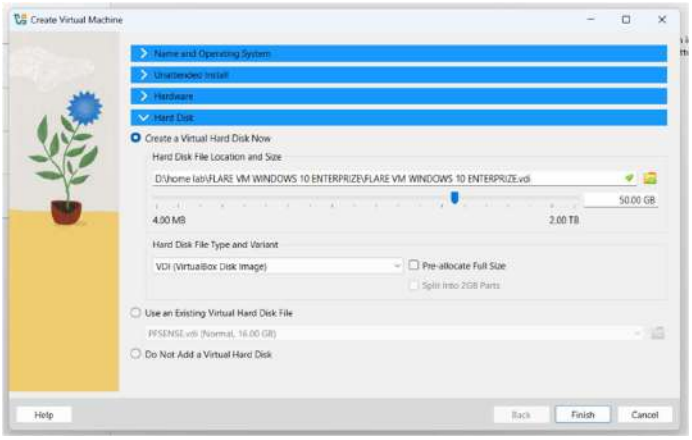
Select Tools from the sidebar and click on **New**.

Give the VM a name. Select the downloaded Windows 10 ISO Image. Check "Skip Unattended Installation". Then click on **Next**.



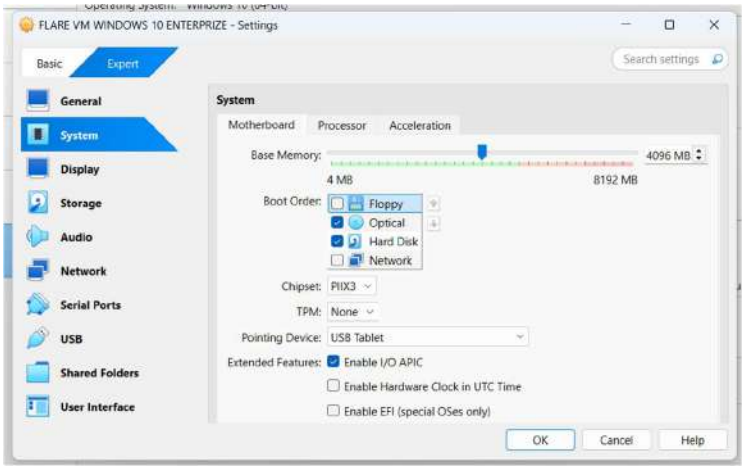
Increase Base Memory to **4096MB** and click on **Next**.

Increase the Drive Size to **50GB** and click on **Finish**.

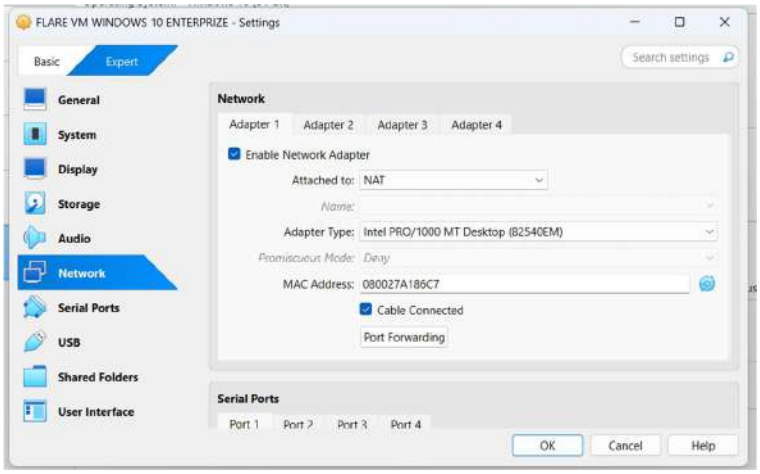


Select the VM then from the toolbar select **Settings**.

Then go to **System -> Motherboard**. In the Boot Order field ensure that **Hard Disk** is on the top followed by **Optical**. Uncheck **Floppy**.



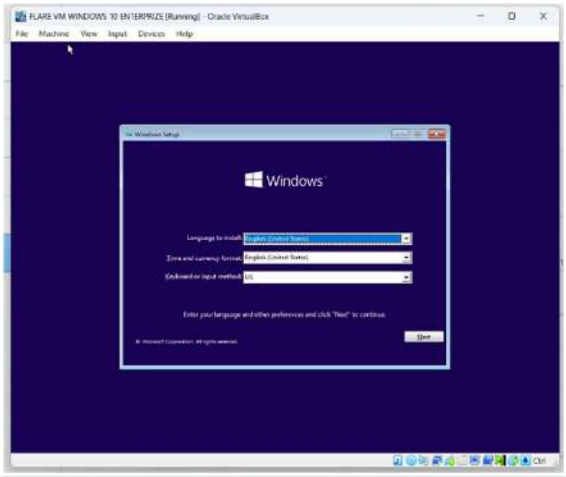
Leave the **Network Adatper** on its default setting of **NAT**.

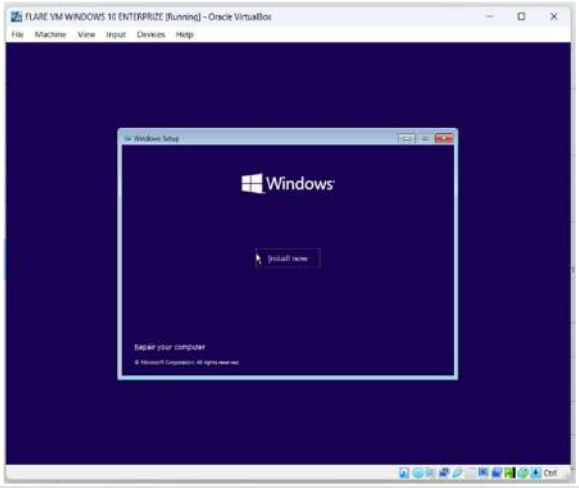


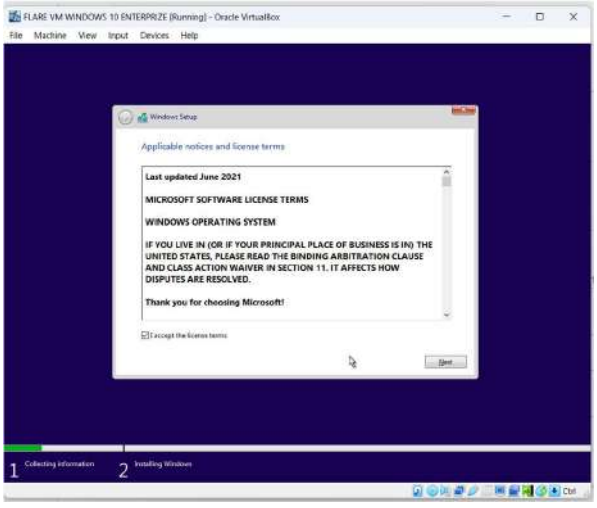
Click on **OK** to save the settings.

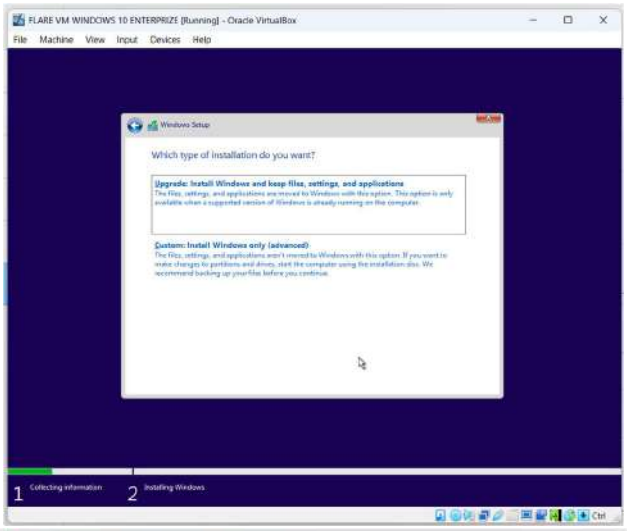
Select the Flare VM from the sidebar and click on **Start**.

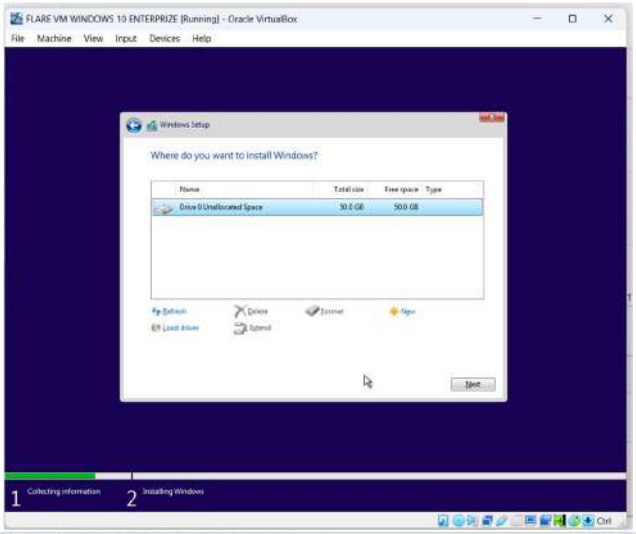
We can follow previous methods for installation.

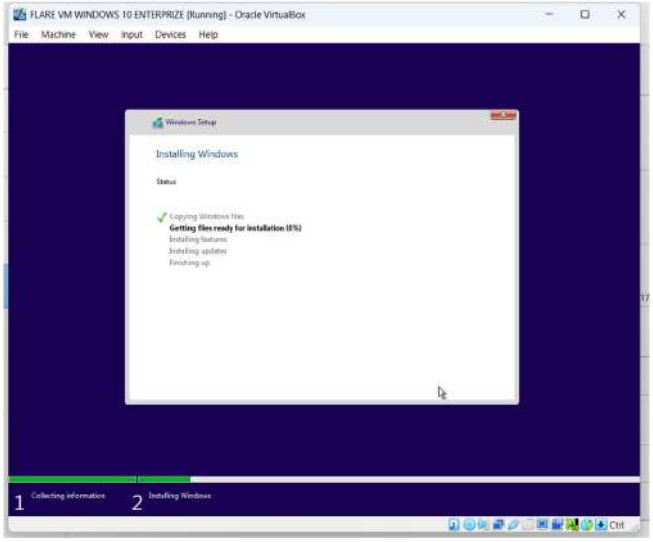


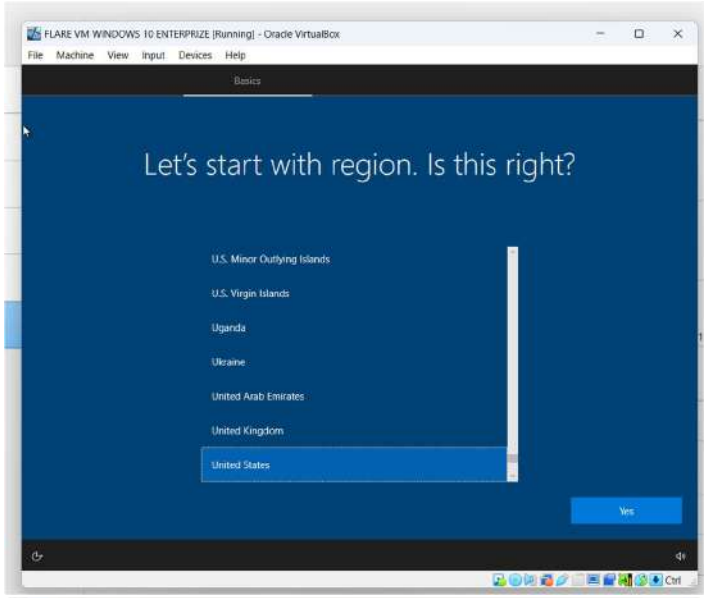


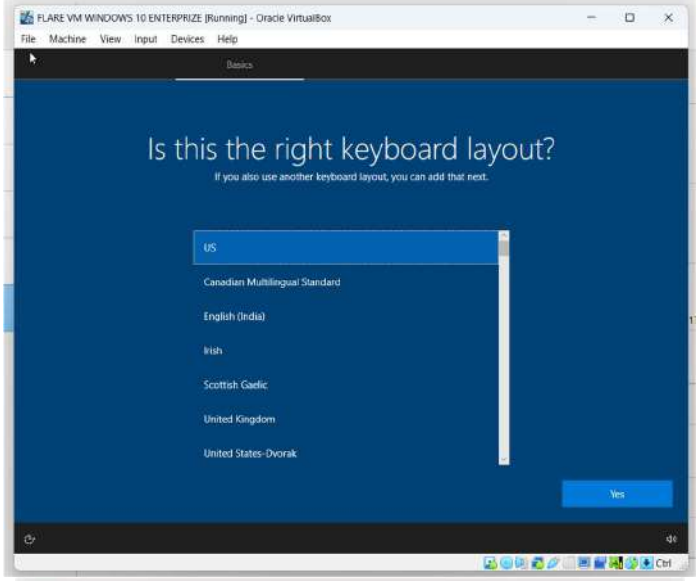


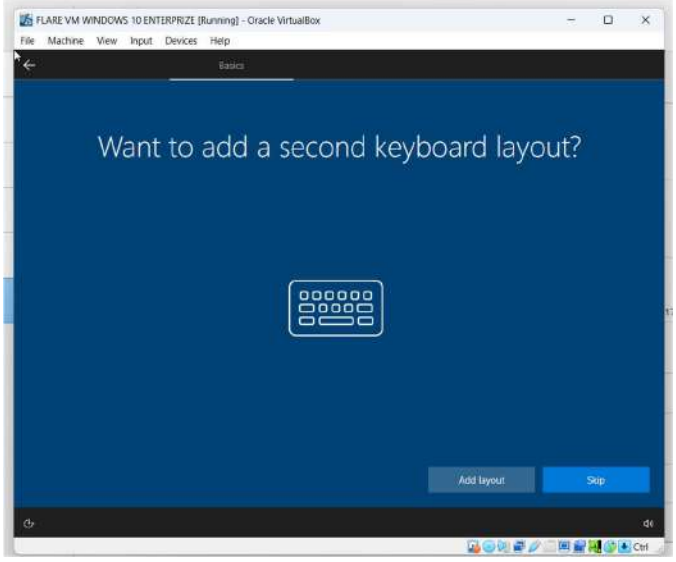

FLARE VM WINDOWS 10 ENTERPRIZE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Windows Setup
Which type of installation do you want?
Upgrade: Install Windows and keep files, settings, and applications
Custom: Install Windows only (advanced)
1 Collecting information
2 Installing Windows


FLARE VM WINDOWS 10 ENTERPRIZE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Windows Setup
Where do you want to install Windows?
Name
Total size
Free space
Type
Drive 0 Unallocated Space
50.0 GB
50.0 GB
Refresh
Delete
Format
New
Load driver
Extend
Next
1 Collecting information
2 Installing Windows

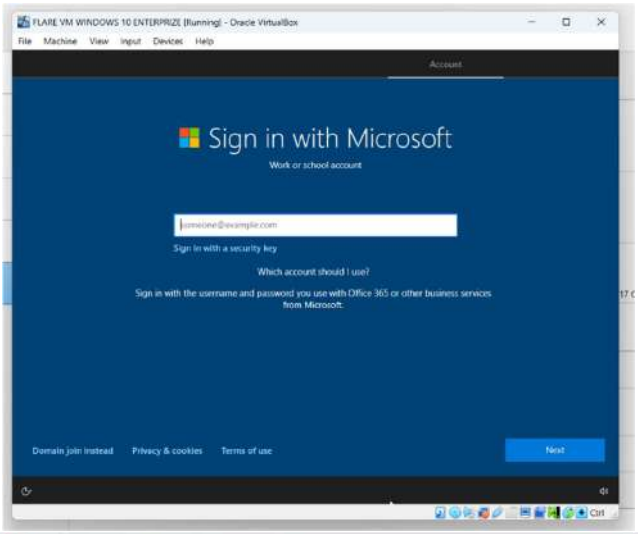

FLARE VM WINDOWS 10 ENTERPRIZE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Windows Setup
Installing Windows
Status
Copying Windows files
Getting files ready for installation (6%)
Installing features
Installing updates
Finishing up
1 Collecting information
2 Installing Windows

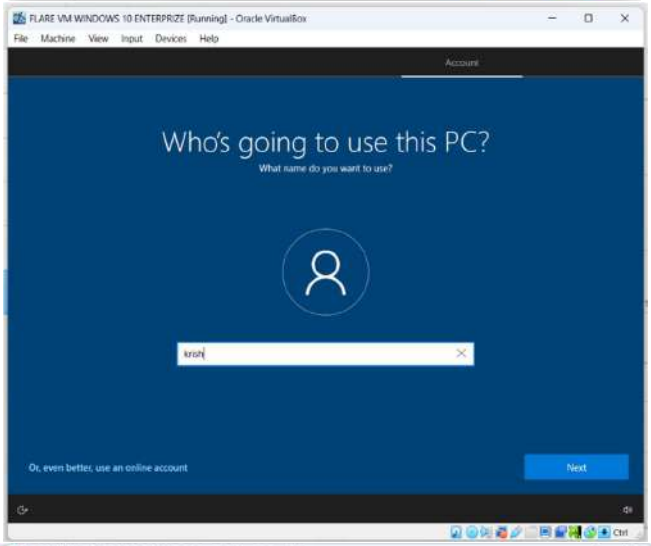

FLARE VM WINDOWS 10 ENTERPRIZE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Basics
Let's start with region. Is this right?
U.S. Minor Outlying Islands
U.S. Virgin Islands
Uganda
Ukraine
United Arab Emirates
United Kingdom
United States
Yes
Ctrl

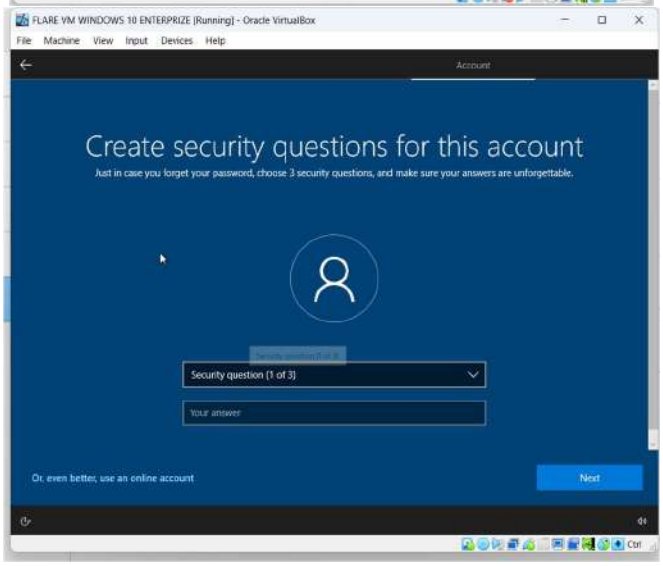

FLARE VM WINDOWS 10 ENTERPRIZE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Basics
Is this the right keyboard layout?
If you also use another keyboard layout, you can add that next.
US
Canadian Multilingual Standard
English (India)
Irish
Scottish Gaelic
United Kingdom
United States-Dvorak
Yes
Ctrl

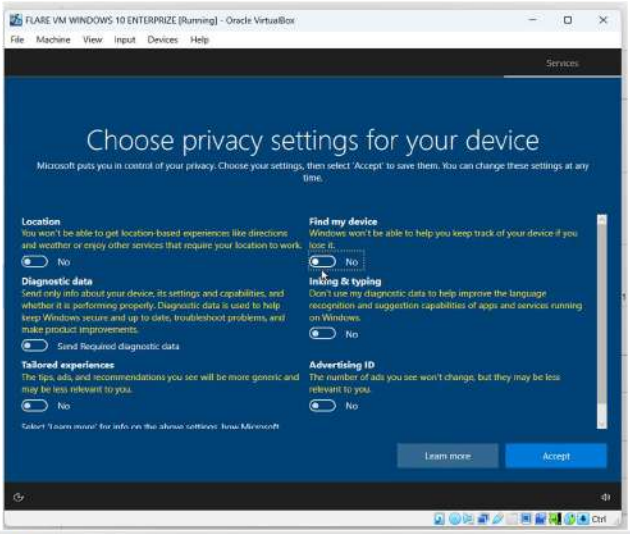

FLARE VM WINDOWS 10 ENTERPRIZE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Basics
Want to add a second keyboard layout?
Add layout
Skip
Ctrl

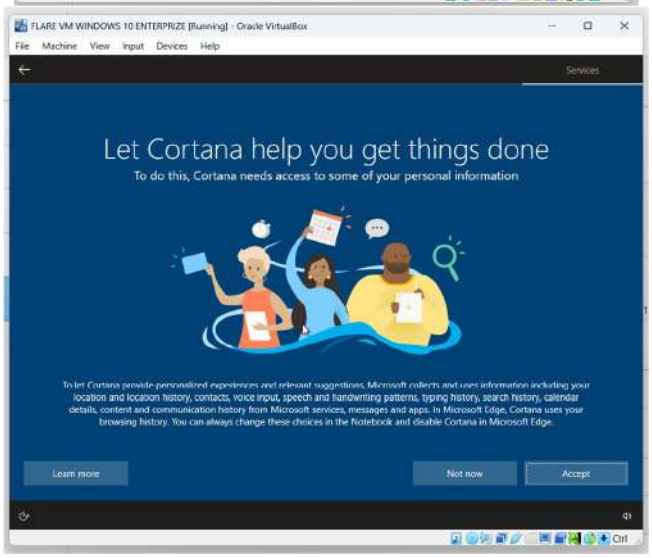
Select “Domain join instead”.



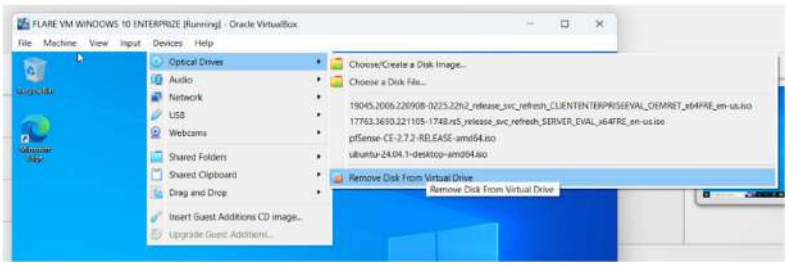


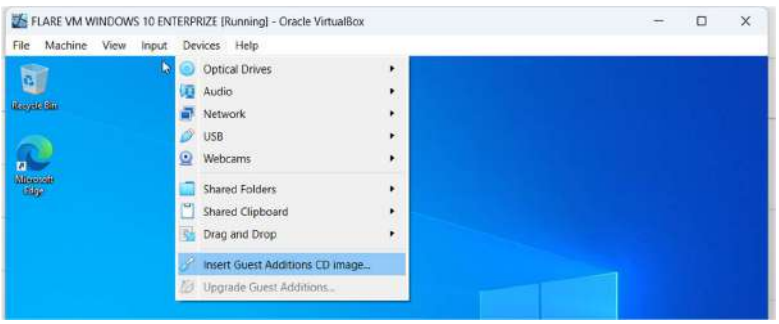


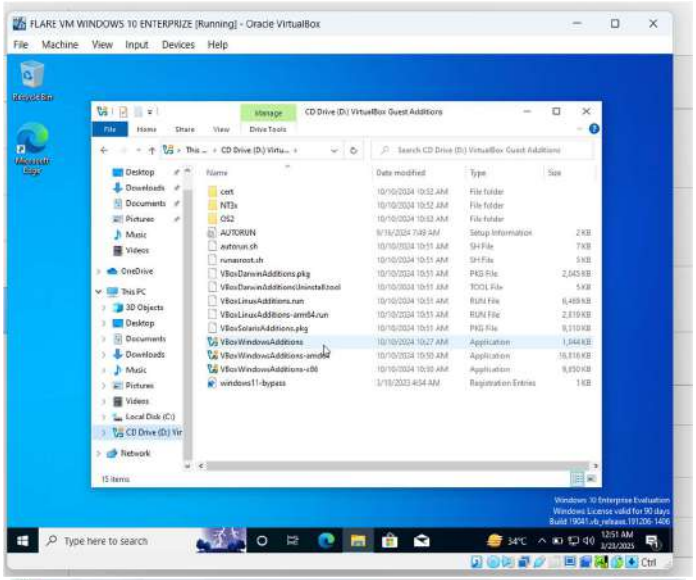


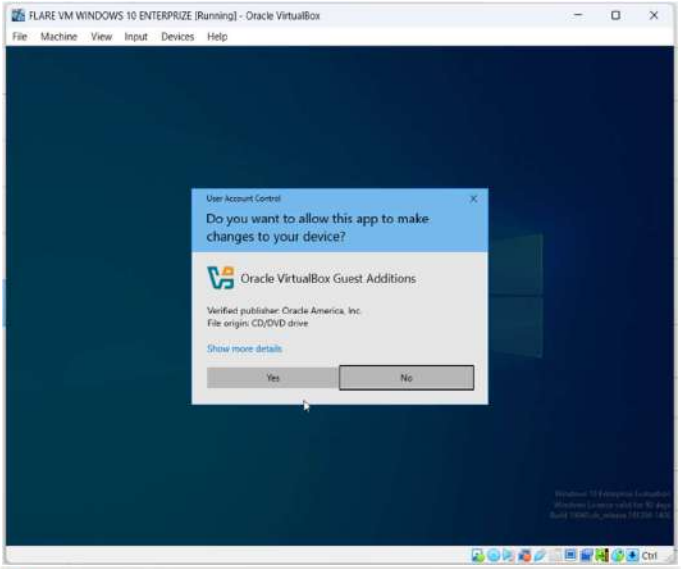


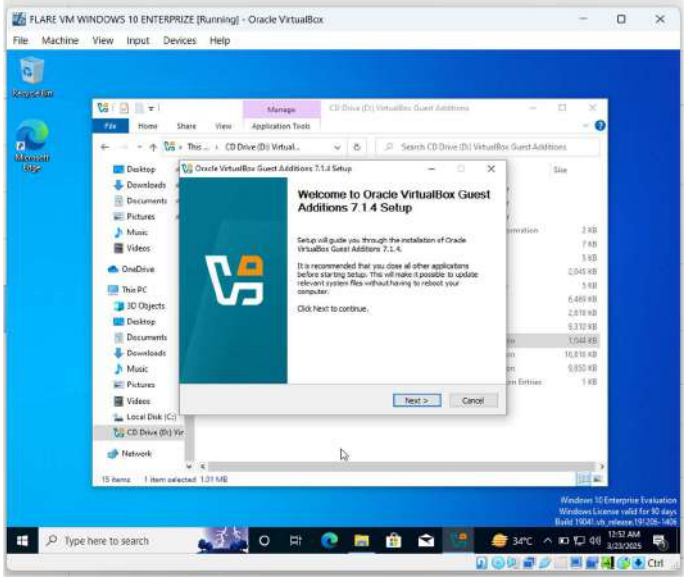
Install Guest Additions to enable the resizing on the VM display.

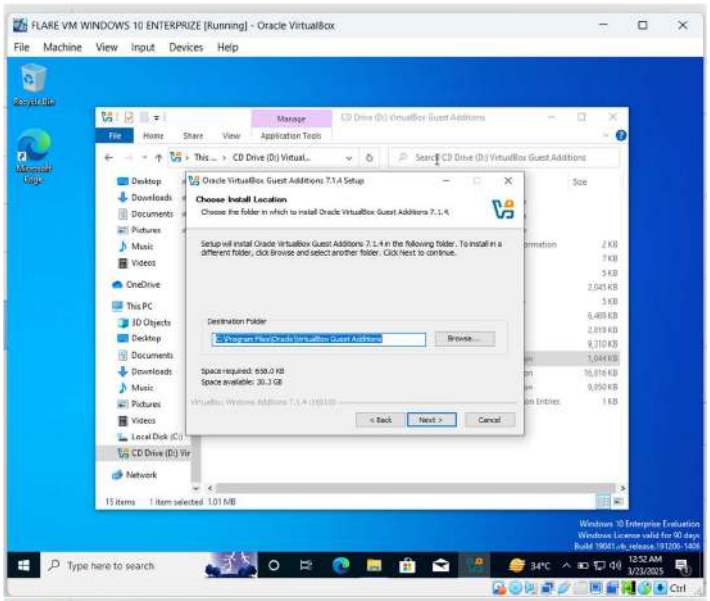


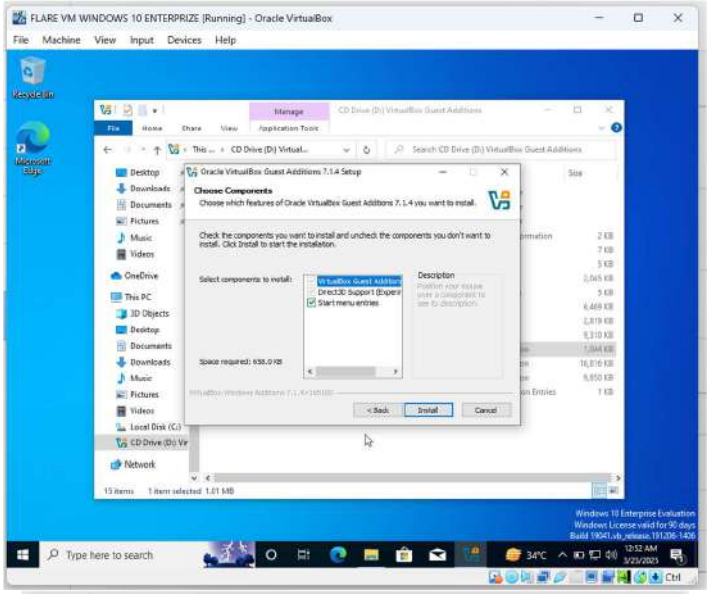


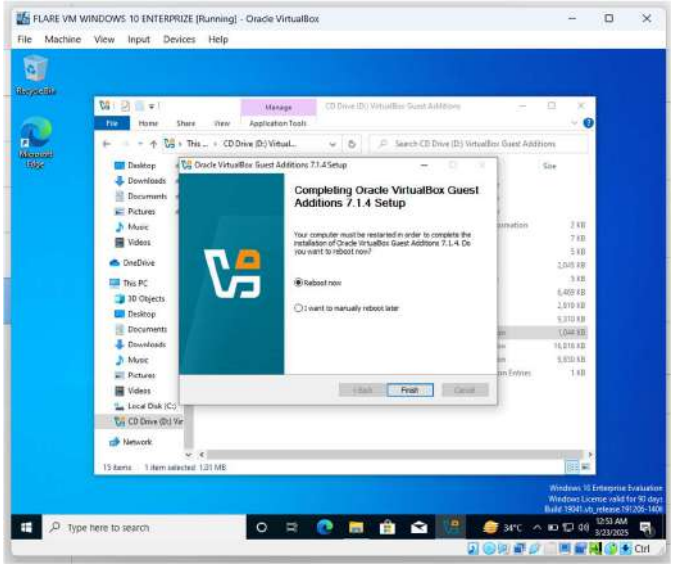

FLARE VM WINDOWS 10 ENTERPRIZE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Type here to search


FLARE VM WINDOWS 10 ENTERPRIZE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
User Account Control
Do you want to allow this app to make changes to your device?
Oracle VirtualBox Guest Additions
Verified publisher: Oracle America, Inc.
File origin: CD/DVD drive
Show more details
Yes
No

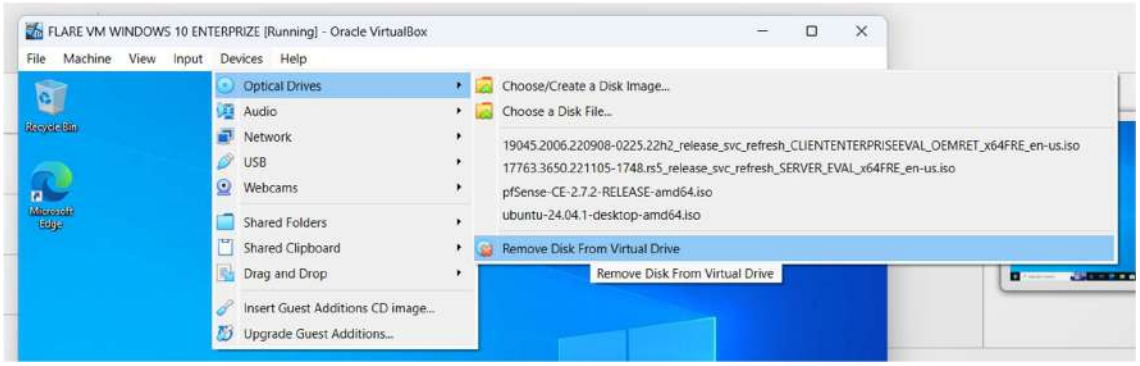

FLARE VM WINDOWS 10 ENTERPRIZE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Welcome to Oracle VirtualBox Guest Additions 7.1.4 Setup
Next >
Cancel
Type here to search


FLARE VM WINDOWS 10 ENTERPRIZE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Oracle VirtualBox Guest Additions 7.1.4 Setup
Choose Install Location
Choose the folder in which to install Oracle VirtualBox Guest Additions 7.1.4.
Setup will install Oracle VirtualBox Guest Additions 7.1.4 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
Destination Folder
Browse...
Space required: 638.0 KB
Space available: 30.1 GB
< Back
Next >
Cancel
Type here to search


FLARE VM WINDOWS 10 ENTERPRIZE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Oracle VirtualBox Guest Additions 7.1.4 Setup
Choose Components
Choose which features of Oracle VirtualBox Guest Additions 7.1.4 you want to install.
Check the components you want to install and uncheck the components you don't want to install. Click Install to start the installation.
Select components to install:
Description
Space required: 638.0 KB
< Back
Install
Cancel
Type here to search

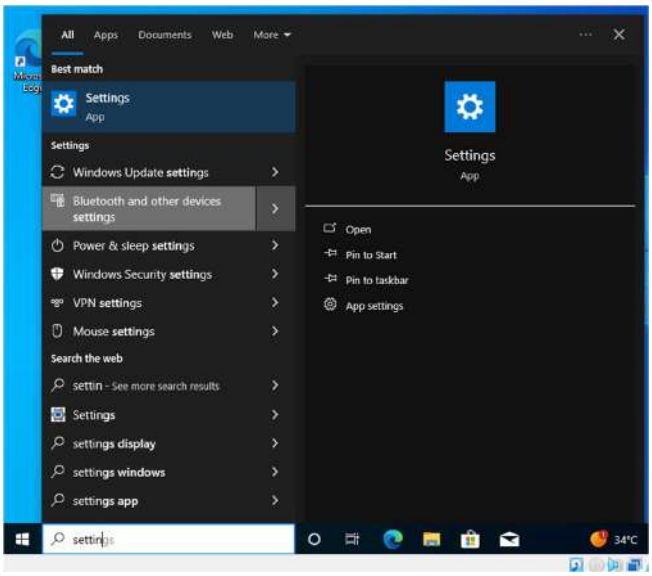

FLARE VM WINDOWS 10 ENTERPRIZE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Oracle VirtualBox Guest Additions 7.1.4 Setup
Completing Oracle VirtualBox Guest Additions 7.1.4 Setup
Your computer must be restarted in order to complete the installation of Oracle VirtualBox Guest Additions 7.1.4. Do you want to reboot now?
Reboot now
I want to manually reboot later
Finish
Type here to search

After rebooting the VM. Remove the Guest Addition Image.

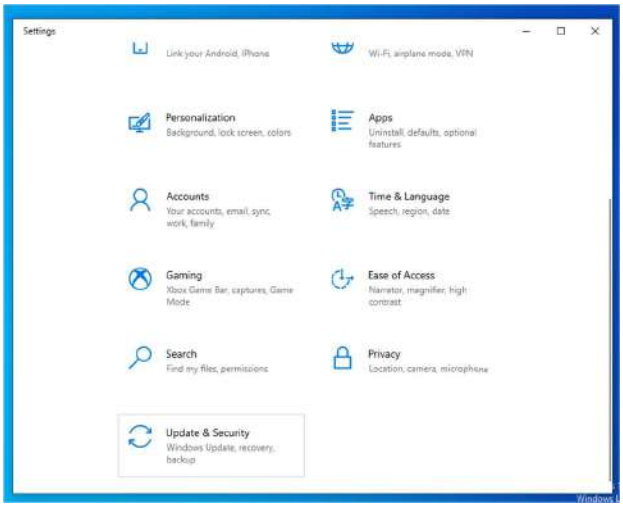


Disabling Windows Update

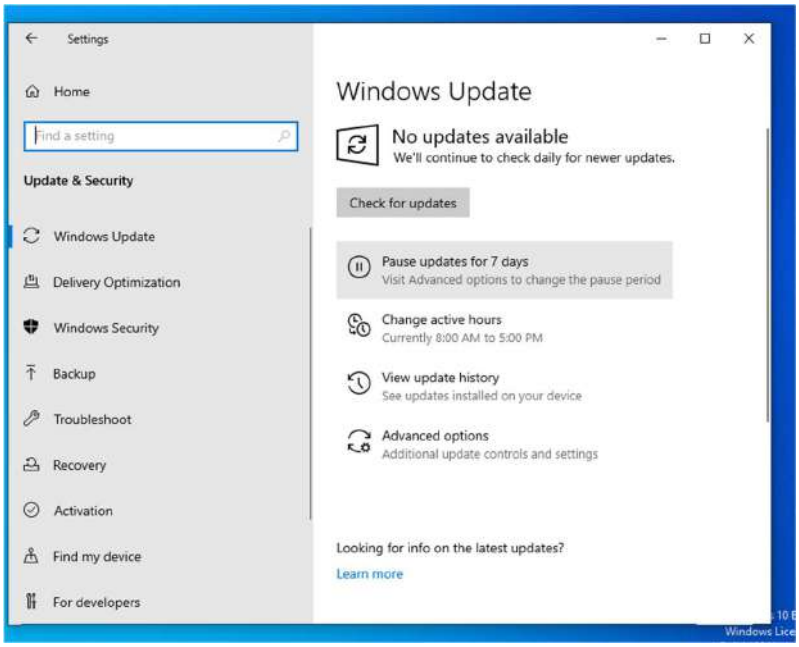
Open on Search bar and search for "Settings". Open the Settings app.



Click on "Update & Security"



Click on the “Pause updates for 7 days” button.

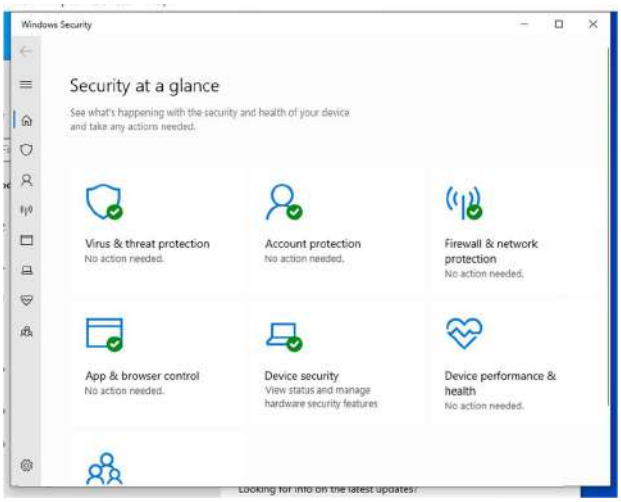


Disabling Windows Defender

Download the following script: jeremybeaume/tools: Script to disable Windows Defender

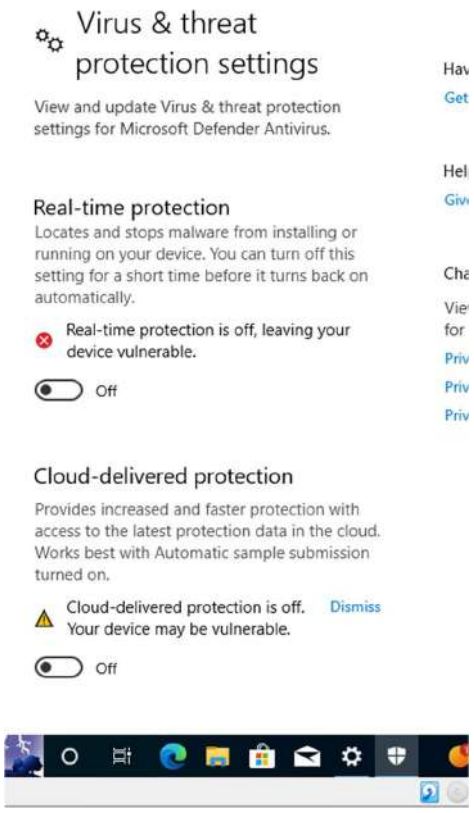
Right-click on the Shield icon on the taskbar and select “View Security Dashboard”.

Click on “Virus & threat protection”.

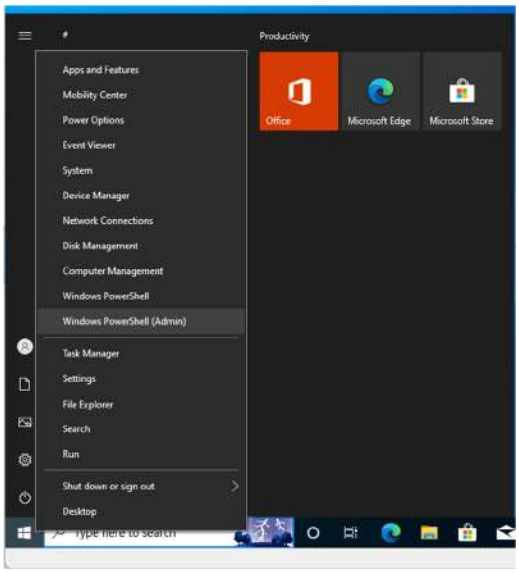


Select “Manage settings” from the “Virus & threat protection settings” section.

Disable all the features that are enabled:



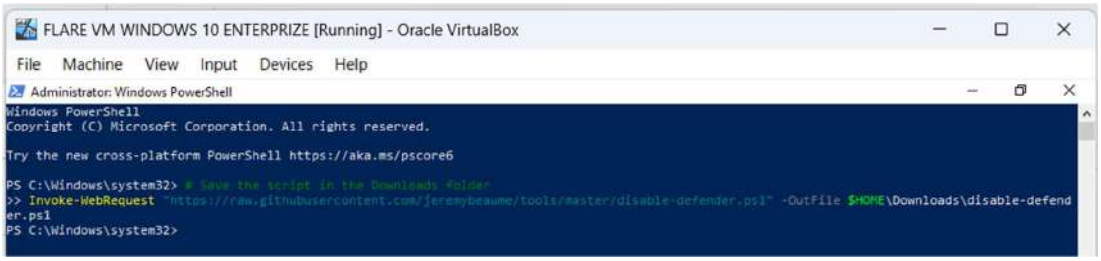
Right-click on the Start menu and select “Windows PowerShell (Admin)”.



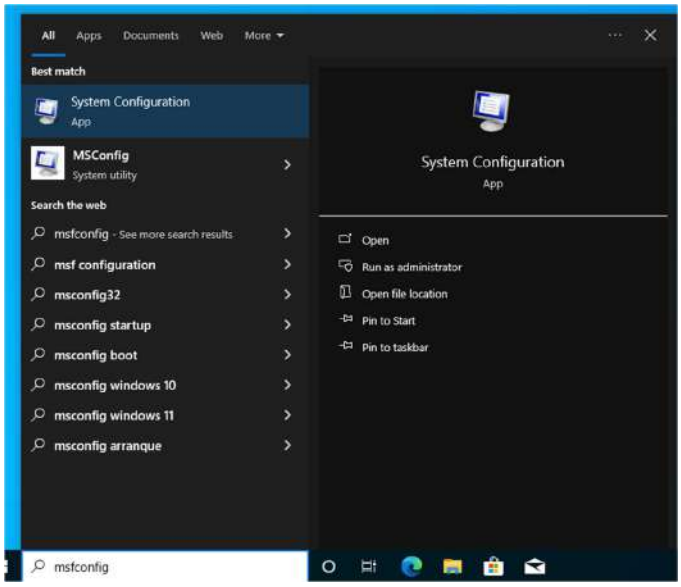
Run the following command to download the script:

Save the script in the Downloads folder

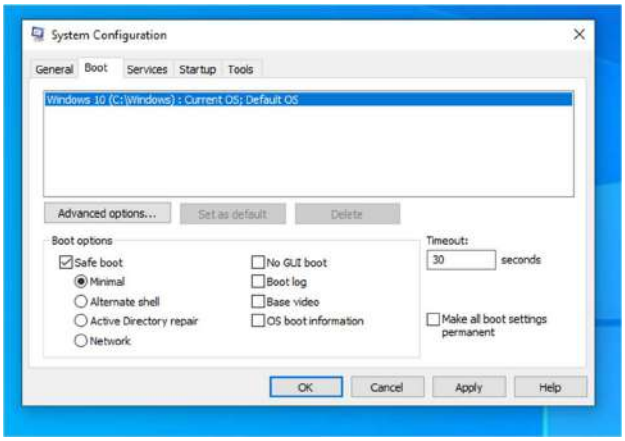
Invoke-WebRequest "https://raw.githubusercontent.com/jeremybeaume/tools/master/disable-defender.ps1" -OutFile $HOME\Downloads\disable-defender.ps1



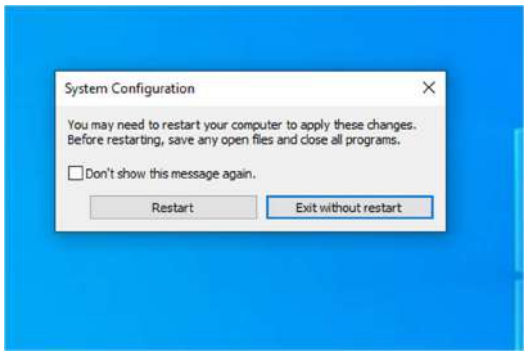
Search msfconfig then **open.**



Navigate to the Boot tab. In the Boot options section enable "Safe boot" and then click on **OK** to save changes.



Click on **Restart** to boot into Safe Mode.

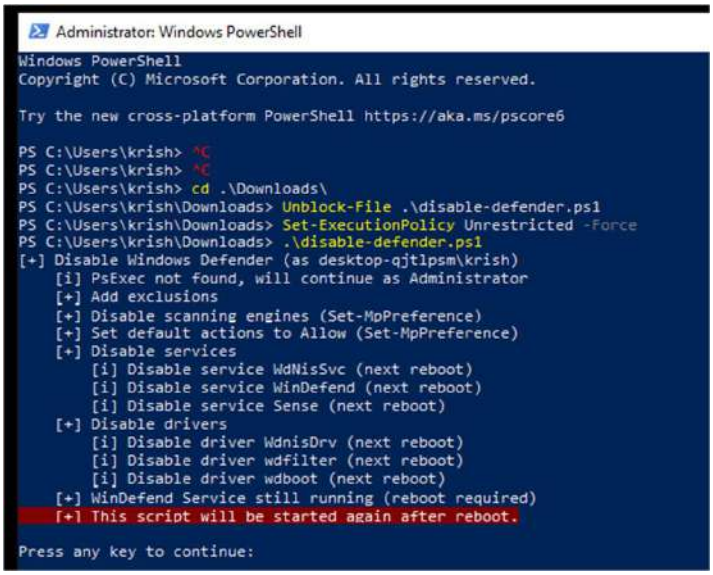


In Safe Mode, the VM cannot be resizable. Safe Mode essentially disables all features that are not required to run the OS.

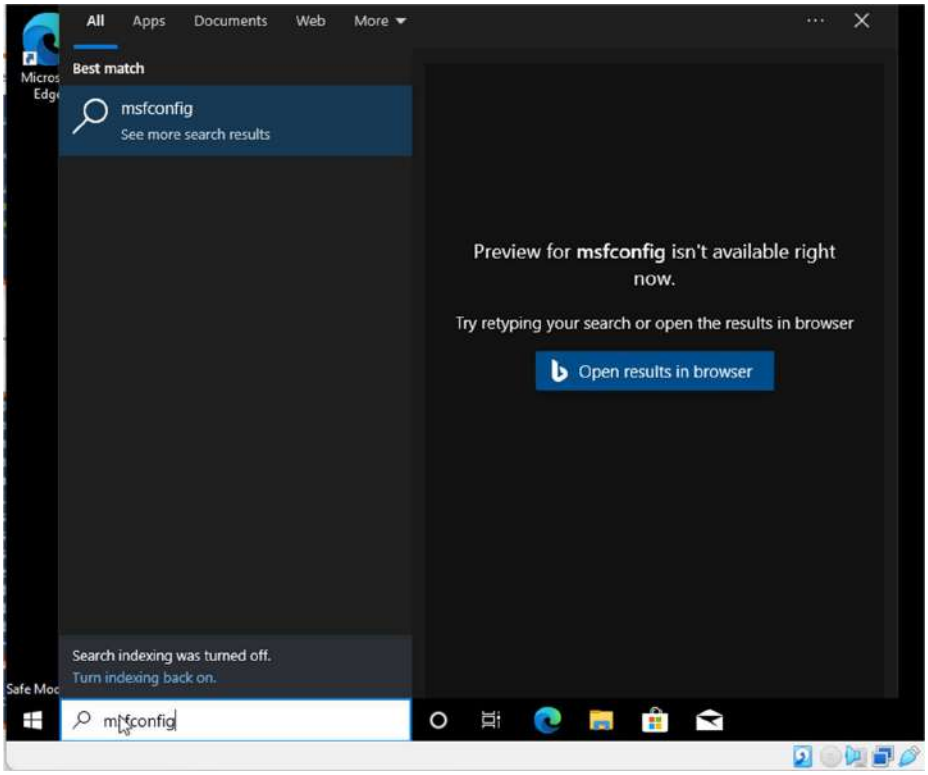
Right-click on the Start menu and select "Windows PowerShell (Admin)" and enter the following commands:

# Change directory	**cd .\Downloads**
# Unblock the downloaded script	**Unblock-File .\disable-defender.ps1**
#Disable the PowerShell policy preventing script execution	
	Set-ExecutionPolicy Unrestricted -Force
# Start the script	**.\disable-defender.ps1**

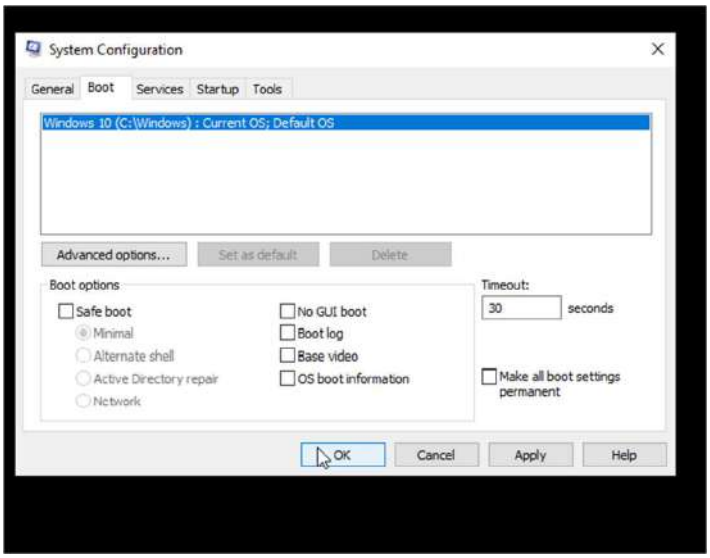
Once the script completes its execution press **Enter** to close the script. Reboot the VM for the changes to take place.



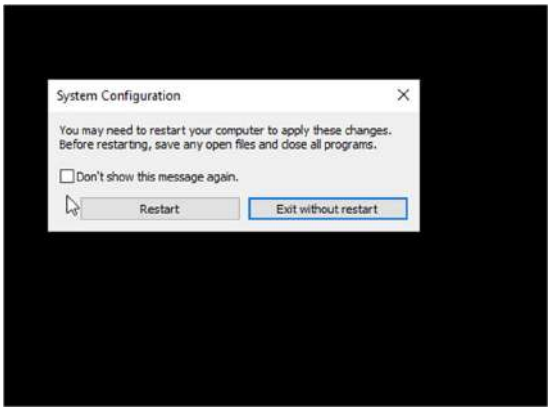
Click on search msconfig and open.



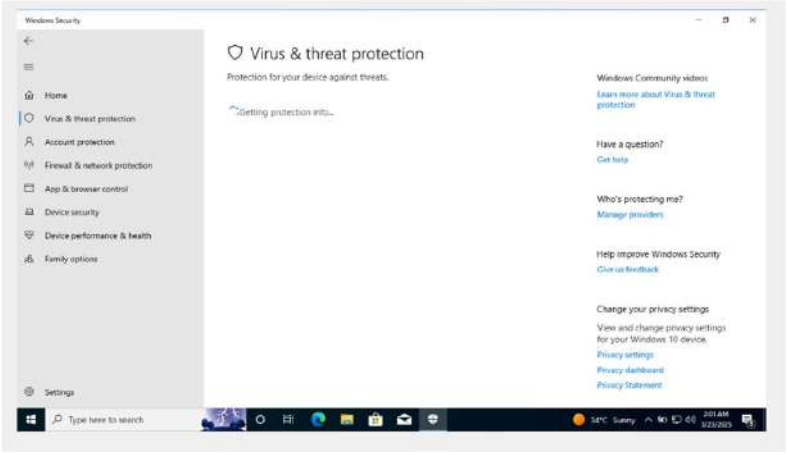
From the Boot options section disable "Safe boot". Click on **Apply** then **OK**.



Then restart computer

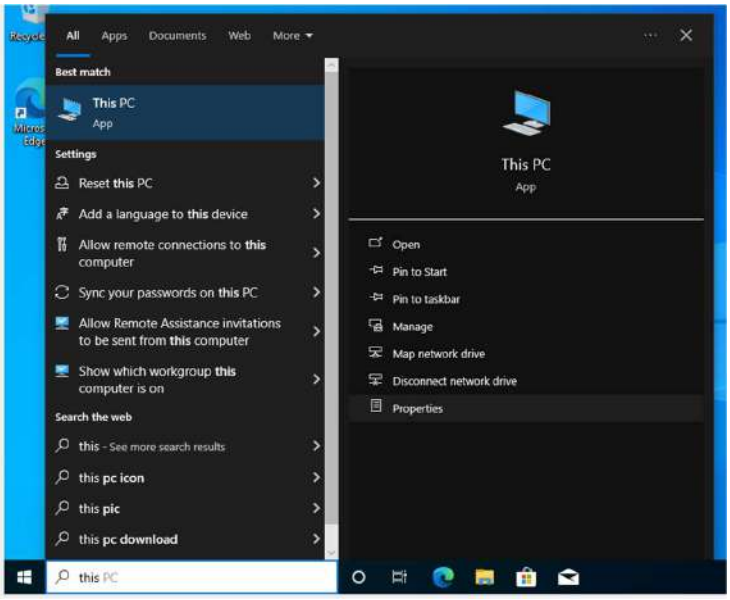


Wait for some time for Defender to load completely and then you will see that "Virus & threat protection" will show as disabled. This means that the script worked successfully.

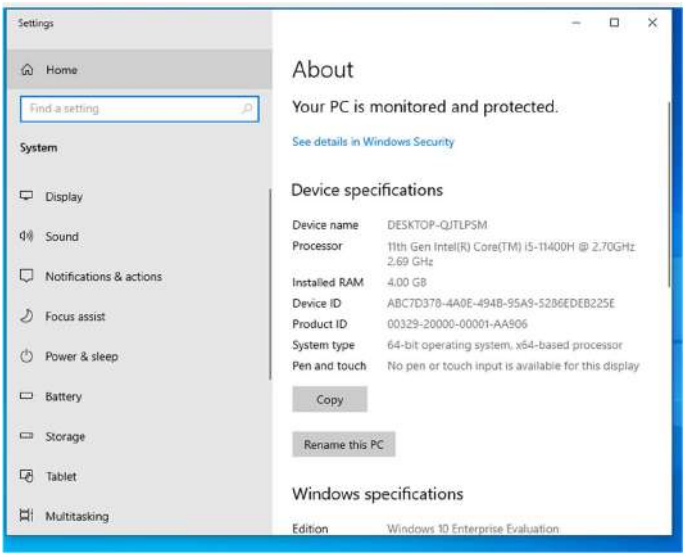


Renaming the VM

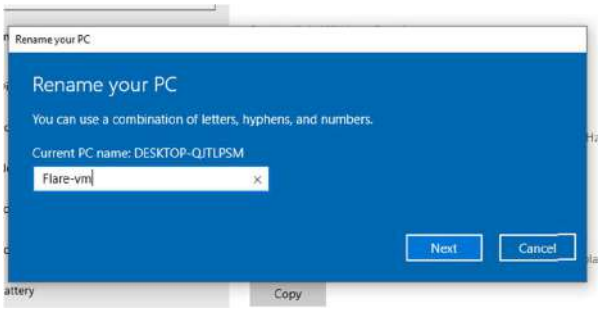
Search for "This PC" and from the right side click on "Properties".



Select "Rename this PC".

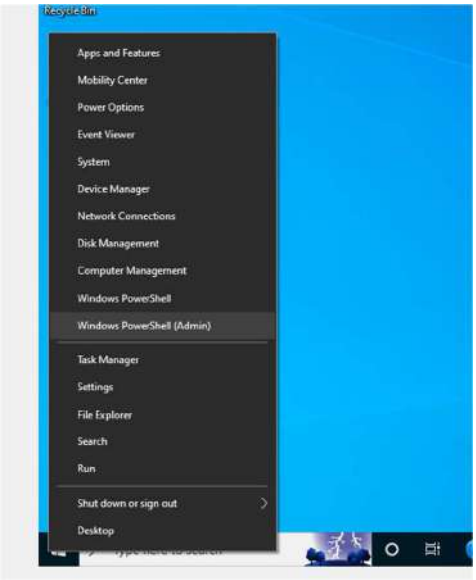


Give the PC a name. Click on **Next** and then select "Restart Now" for the changes to take effect.



Flare VM Installation

Right-click on the Start menu and select “Windows PowerShell (Admin)”.



Enter the following commands to download and run the Flare VM script.

Download the FlareVM script

Invoke-WebRequest "https://raw.githubusercontent.com/mandiant/flare-vm/main/install.ps1" -OutFile $HOME/Downloads/install.ps1

Go to Downloads Folder

cd $HOME/Downloads

Unlock the downlaoded script

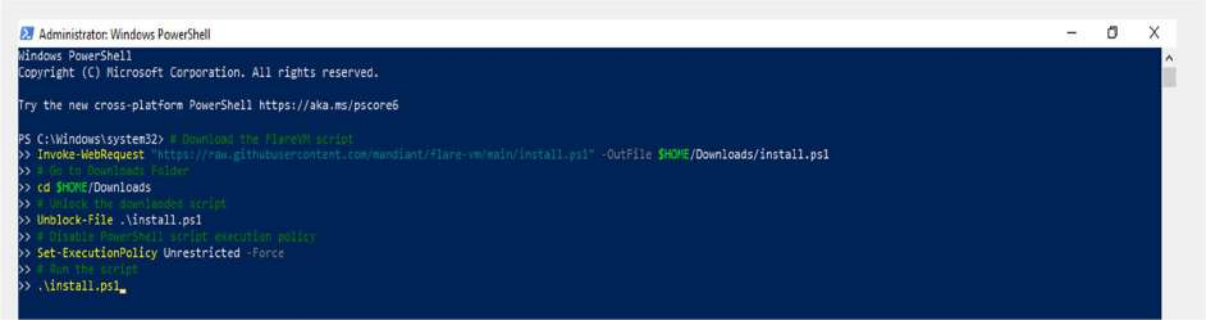
Unblock-File .\install.ps1

Disable PowerShell script execution policy

Set-ExecutionPolicy Unrestricted -Force

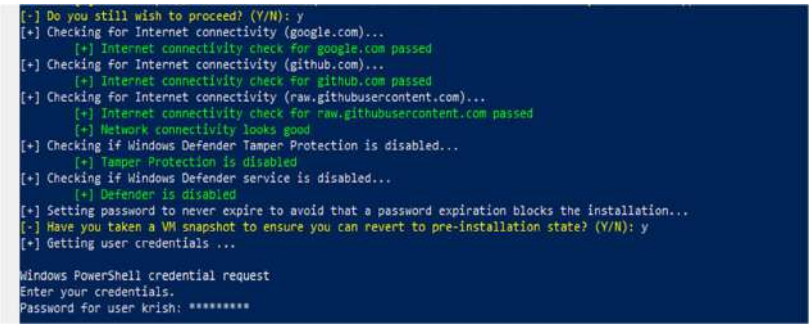
Run the script

.\install.ps1



The script will make some checks before starting the installation.

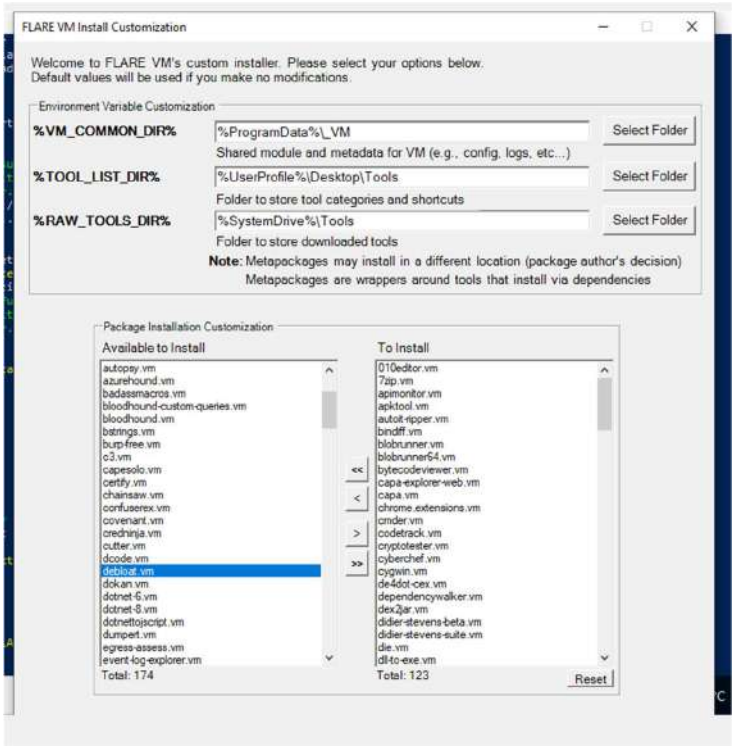
Enter **Y** when asked about Snapshot. Enter password when prompted.



After some time the Flare VM configuration dialog will open.

In the Package Installation Customization section from the left side select "debloat.vm" and click on the right arrow to select it for installation.

Click on **OK** to start the install. The VM will restart multiple times during the setup



The installation can take a very long time. Once the setup is complete we will get the following prompt click on **Finish** to complete the setup.

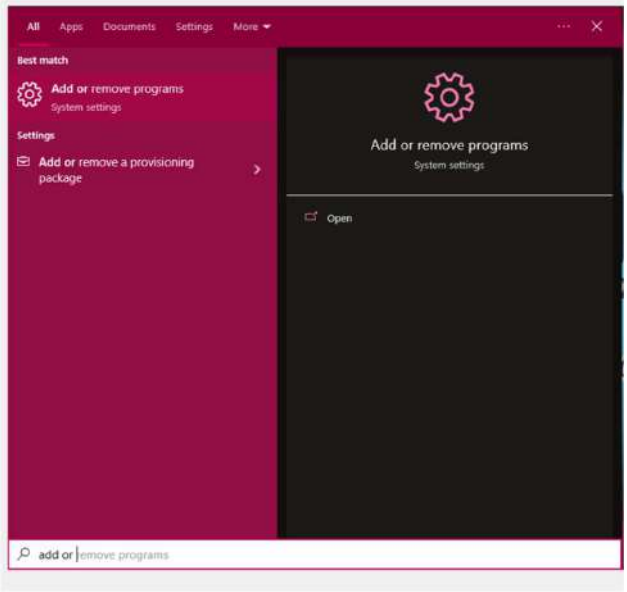
After the installation is complete. Restart the VM to complete the setup.

Post-Install Configuration

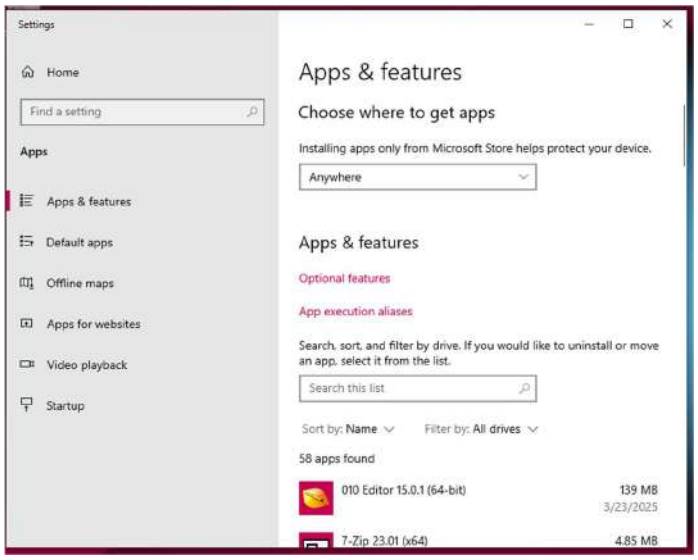
Installing OpenSSH Server

Once we move this VM to the **ISOLATED** subnet it will not be able to access the internet. We will not be able to download malware samples directly from the Internet. We will download the samples onto a different VM that has Internet access and then move them to this machine using SSH. I will cover this process in more detail in a later module. For now, we need to install "OpenSSH Server".

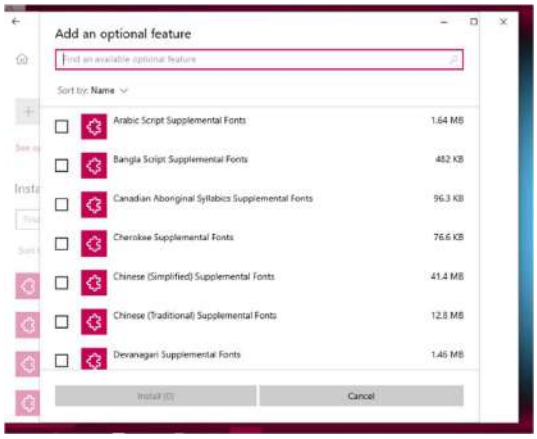
Open the Search bar. Type "Add" and from the results select the "Add or remove programs" option.



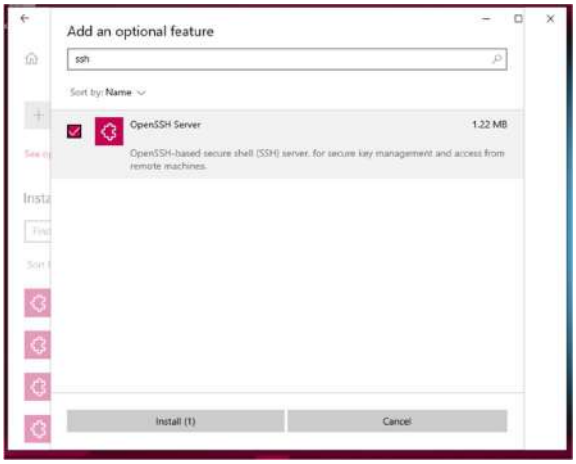
Click on **Optional Features** under "Apps & features".



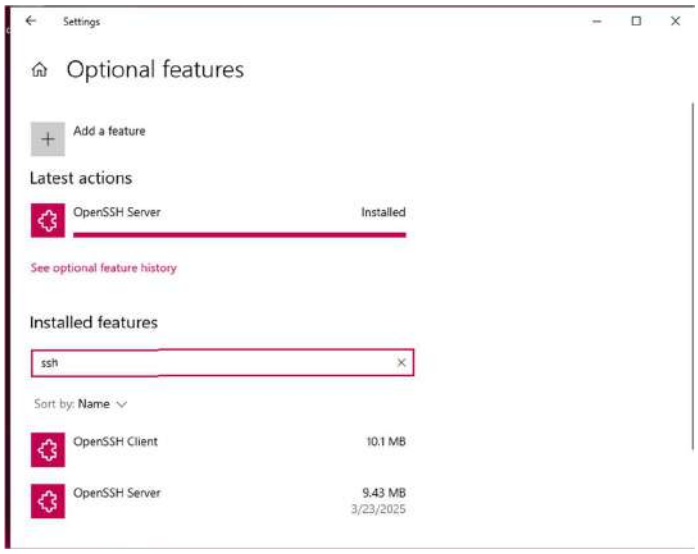
Click on **Add a feature**. This will open a new menu.



Search for "SSH". Enable "OpenSSH Server" and then click on **Install**.

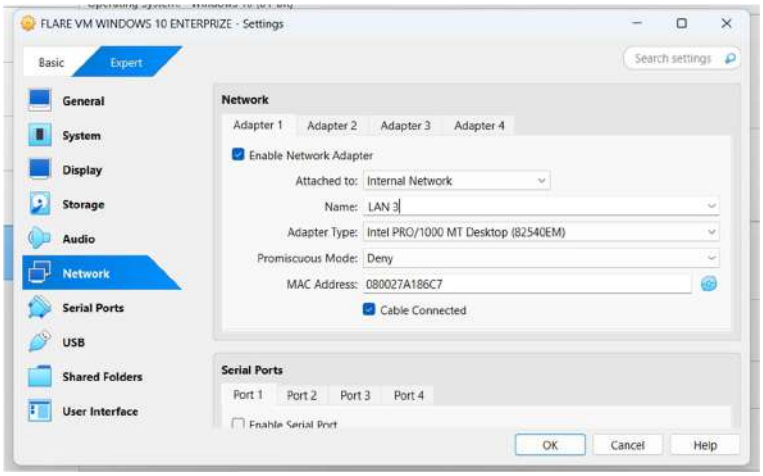


Once the install is complete if you search for "SSH" in the "Installed features" section you should see "OpenSSH Client" and "OpenSSH Server".



Moving VM to the Isolated Network

Shut down the VM. Open the VM **Settings** page and go to **Network**. For the Attached to field select **Internal Network**. For name select **LAN 3**. Click on **OK** to save the changes.



SPLUNK SETUP

deploying the VM we will create a new Interface in pfSense called Security that will have our DFIR VM and in the future other security tools.

As discussed in the last module using VirtualBox GUI we cannot create more than 4 interfaces but using the CLI we can create up to 8 Interfaces.

Before creating the interface we need the name of the pfSense VM. In my case, the VM is called "PFSENSE". Also, ensure the VM is "Powered Off" before running the commands.

The last Adapter we created is called Adapter 5.

Launch PowerShell and run the following commands:

Create a Internet Network

VBoxManage modifyvm "PFSENSE" --nic6 intnet

Use the Paravirtualized Adapter

VBoxManage modifyvm "PFSENSE" --nictype6 virtio

Give it the name LAN 3

VBoxManage modifyvm "PFSENSE" --intnet6 "LAN 4"

Network Interface is connected by Cable

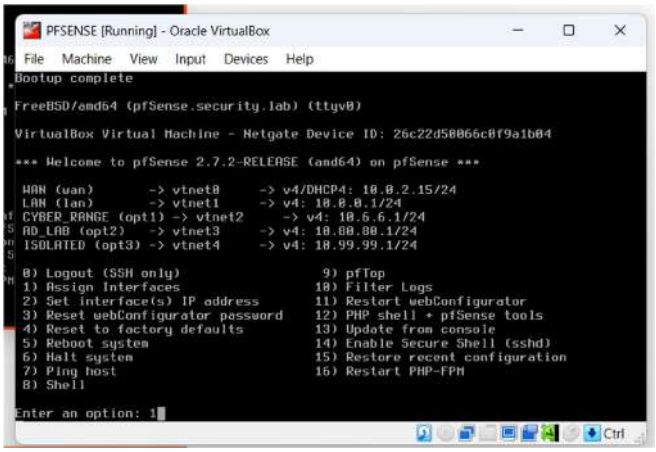
VBoxManage modifyvm "PFSENSE" --cableconnected6 on

```
PS C:\Users\rajgu> VBoxManage modifyvm "PFSENSE" --nic6 intnet
PS C:\Users\rajgu> VBoxManage modifyvm "PFSENSE" --nictype6 virtio
PS C:\Users\rajgu> VBoxManage modifyvm "PFSENSE" --intnet6 "LAN 4"
PS C:\Users\rajgu> VBoxManage modifyvm "PFSENSE" --cableconnected6 on
PS C:\Users\rajgu>
```

The pfSense VM will now have an Adapter 6.

Enabling the Interface

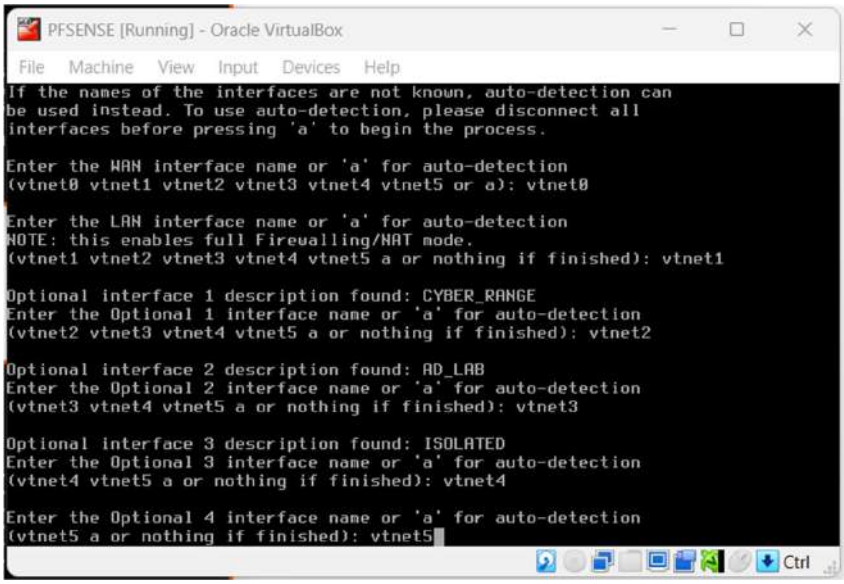
Start the pfSense VM. pfSense will not detect the new interface. We need to onboard the interface before it shows up.



Enter **1** to select “Assign Interfaces”.
Should VLANs be set up now? **n**

```
Enter an option: 1


Valid interfaces are:

vtnet0  08:00:27:3b:c7:fe    (up) VirtIO Networking Adapter
vtnet1  08:00:27:39:53:45    (up) VirtIO Networking Adapter
vtnet2  08:00:27:8b:25:a9    (up) VirtIO Networking Adapter
vtnet3  08:00:27:84:66:ac    (up) VirtIO Networking Adapter
vtnet4  08:00:27:fe:d8:4d    (up) VirtIO Networking Adapter
vtnet5  08:00:27:cc:c7:3e (down) VirtIO Networking Adapter

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
```

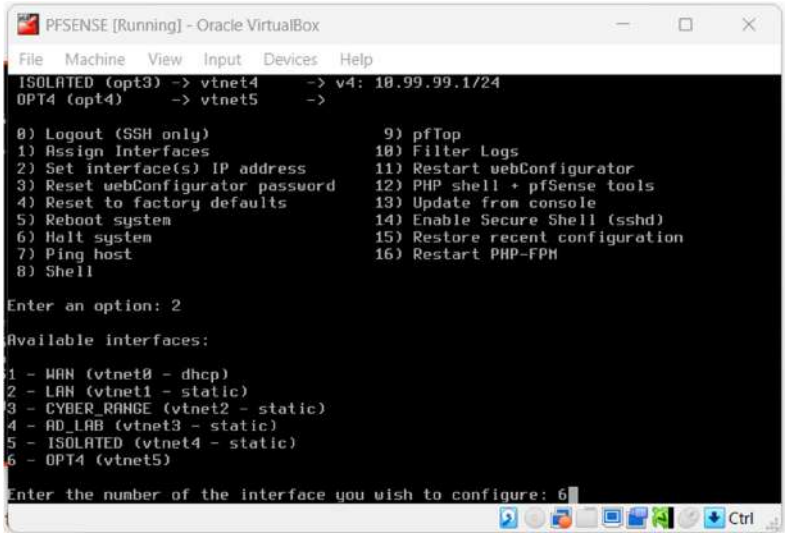
Enter the WAN interface name: **vtnet0**
Enter the LAN interface name: **vtnet1**
Enter the Optional 1 interface name: **vtnet2**
Enter the Optional 2 interface name: **vtnet3**
Enter the Optional 3 interface name: **vtnet4**
Enter the Optional 4 interface name: **vtnet5**



Do you want to proceed?: **y**

The new interface is onboarded. Now we need to assign it an IP address.

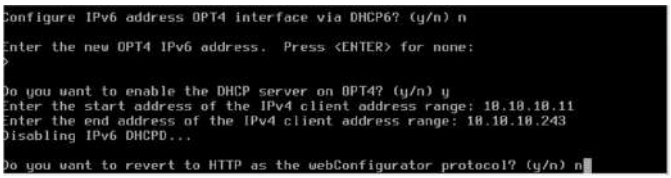
Enter **2** to select "Set interface(s) IP address". Enter **6** to select the OPT4 interface.



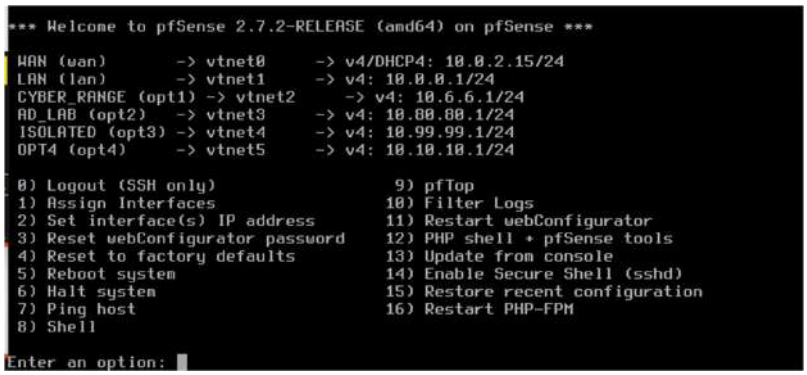
Configure IPv4 address OPT3 interface via DHCP?: **n**
Enter the new OPT4 IPv4 address: **10.10.10.1**
Enter the new OPT4 IPv4 subnet bit count: **24**

For the next question directly press **Enter**. Since this is an **LAN** interface we do not have to worry about configuring the upstream gateway.

Configure IPv6 address OPT4 interface via DHCP6: **n**
For the new OPT4 IPv6 address question press **Enter**.
Do you want to enable the DHCP server on OPT4?: **y**
Enter the start address of the IPv4 client address range: **10.10.10.11**
Enter the end address of the IPv4 client address range: **10.10.10.243**
Do you want to revert to HTTP as the webConfigurator protocol?: **n**

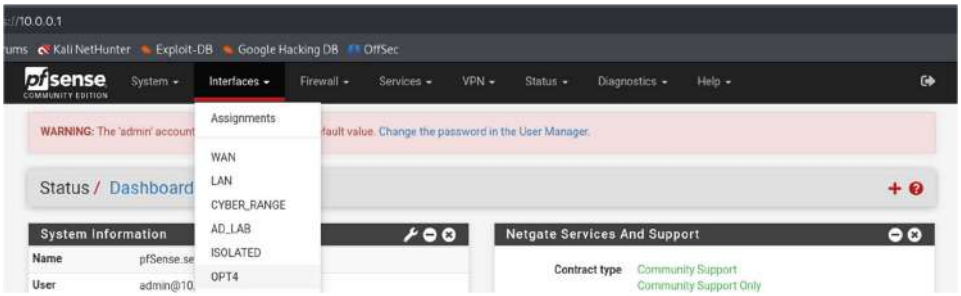


Now interface OPT4 will have an IP address.

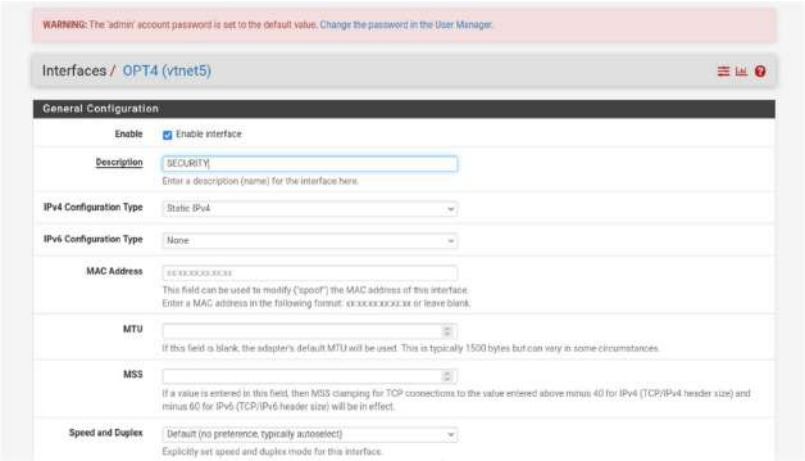


Renaming the Interface

Launch the Kali Linux VM. Login to the pfSense web portal. From the navigation bar select **Interfaces -> OPT4**.



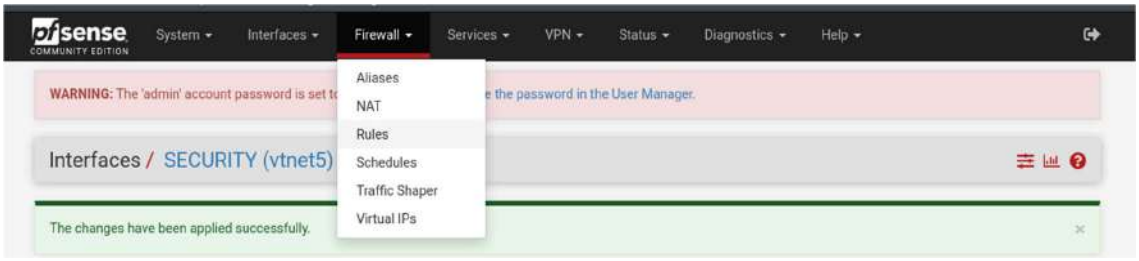
In the description field enter **SECURITY**. Scroll to the bottom and click on **Save**.



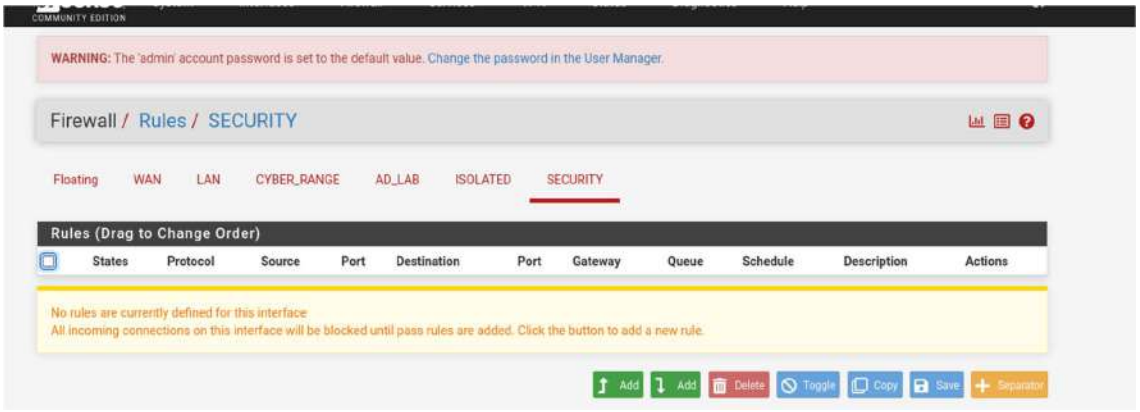
Click on **Apply Changes** in the popup that appears to persist the changes.

Interface Firewall Configuration

From the navigation bar click on **Firewall -> Rules**.

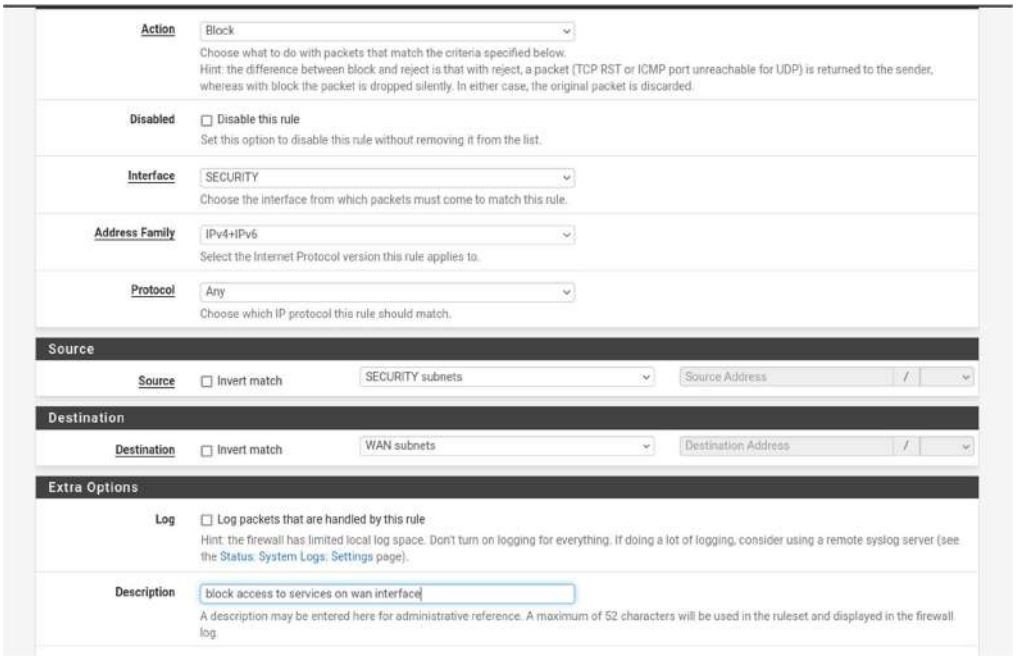


Select the SECURITY tab. Click on the “Add” button to create a new rule.



Change the values as follows:
Action: **Block**
Address Family: **IPv4+IPv6**
Protocol: **Any**
Source: **SECURITY subnets**
Destination: **WAN subnets**
Description: **Block access to services on WAN interface**

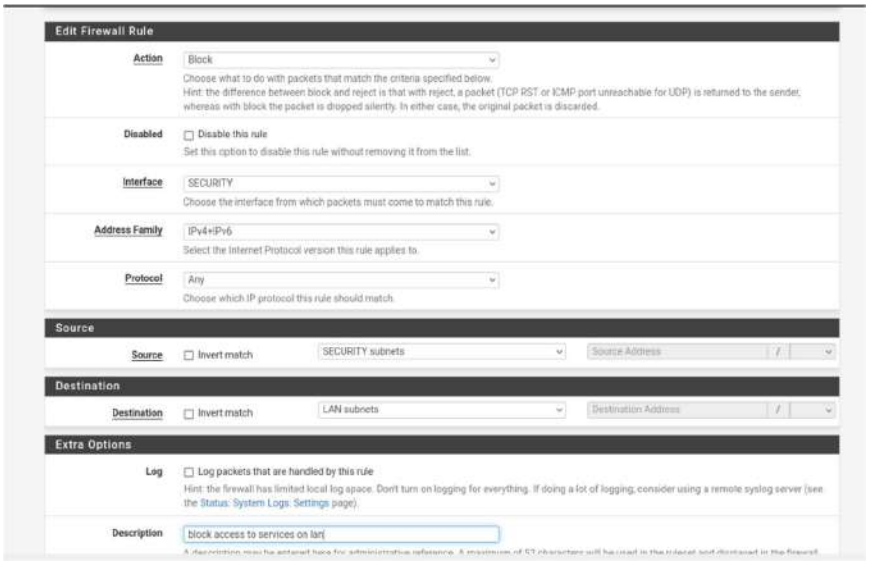
Scroll to the bottom and click on **Save**.



Ignore the popup for saving changes. Click on “Add” to create a new rule.

Change the values as follows:
Action: **Block**
Address Family: **IPv4+IPv6**
Protocol: **Any**
Source: **SECURITY subnets**
Destination: **LAN subnets**
Description: **Block access to services on LAN**

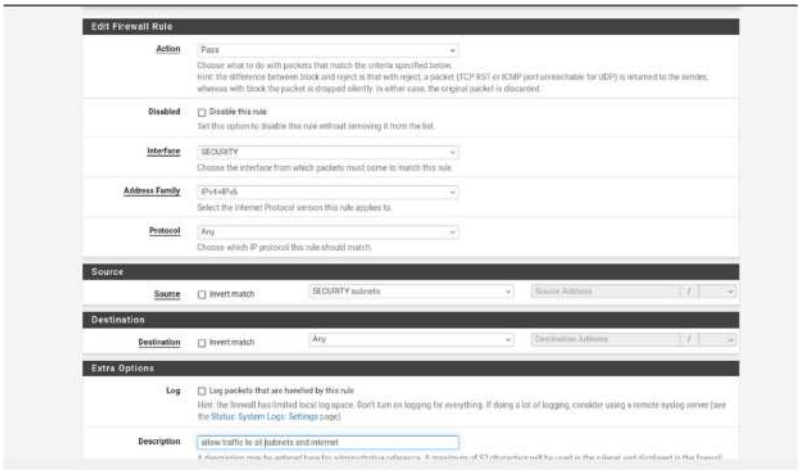
Scroll to the bottom and click on **Save**.



Click on “Add” to create a new rule.

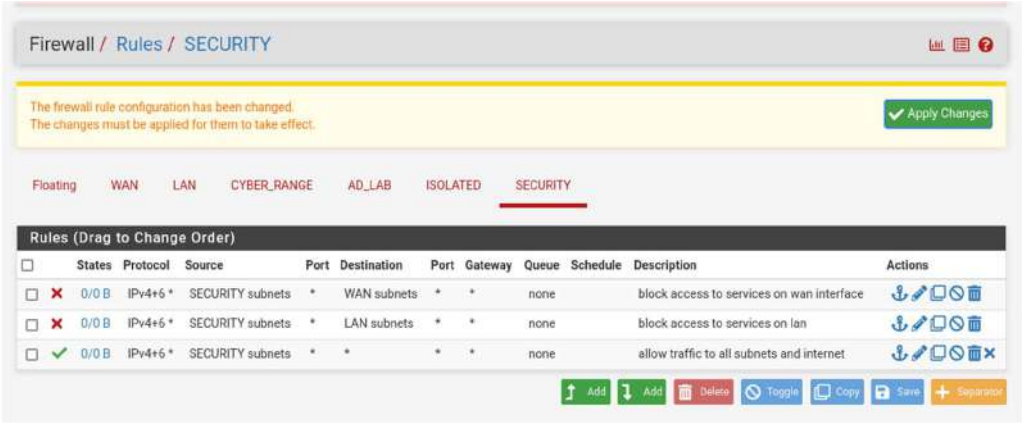
Change the values as follows:
Address Family: **IPv4+IPv6**
Protocol: **Any**
Source: **SECURITY subnets**
Description: **Allow traffic to all subnets and Internet**

Scroll to the bottom and click on **Save**.

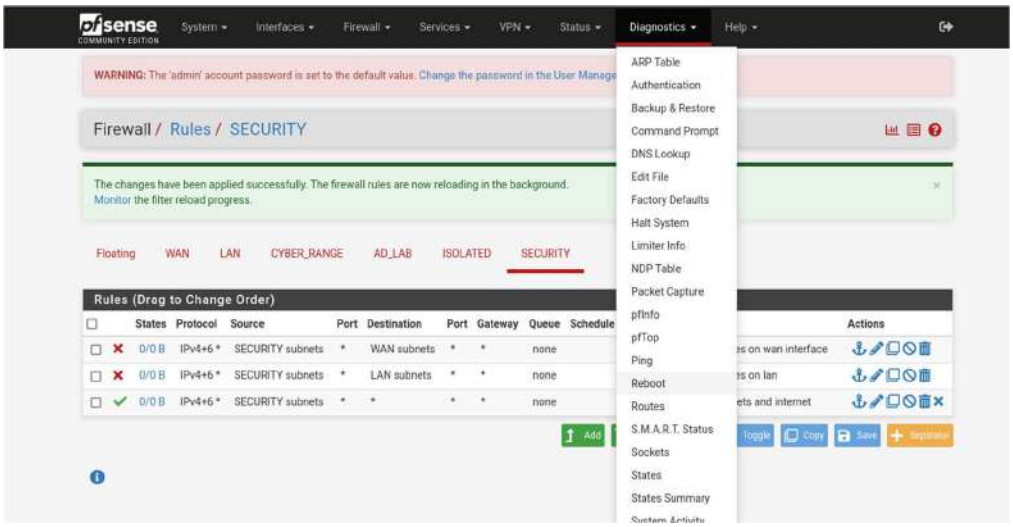


In the popup click on **Apply Changes** to persist the new rule.

The final result will be as follows:

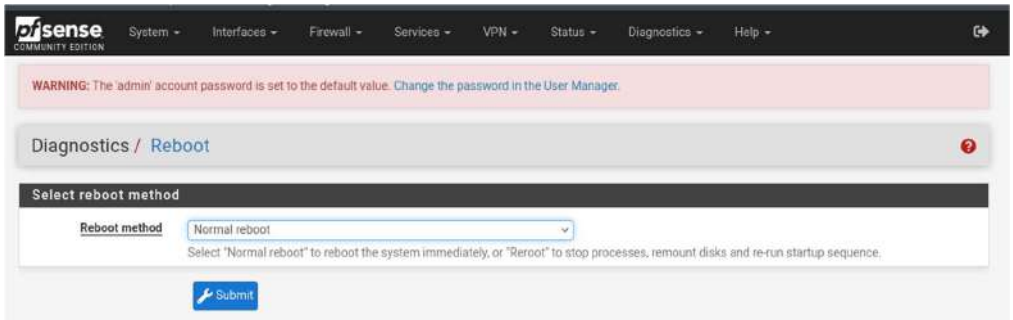


Now we need to restart pfSense to ensure that the firewall rules are propagated properly. From the navigation bar select **Diagnostics -> Reboot**.



Click on **Submit**.

Once pfSense boots up you will be redirected to the login page.



In this module, we will set up Splunk (SIEM) in a Ubuntu VM. The VM will be added to the SECURITY subnet. Then we will configure Splunk Universal Forwarder on our Windows Server 2019 (DC) VM which will allow Splunk to ingest logs from the DC.

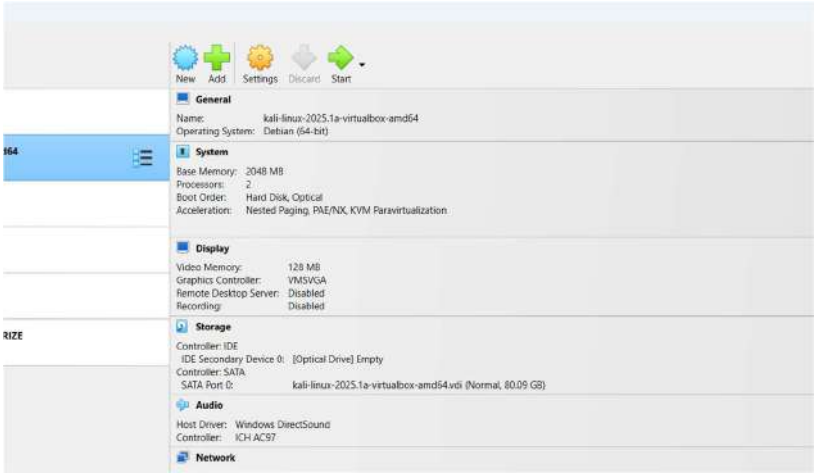
Downloading the Image

Go to the following URL: Download Ubuntu Desktop | Download | Ubuntu.
Download the latest LTS version of Ubuntu. As of writing the latest version is **2022.04.3**

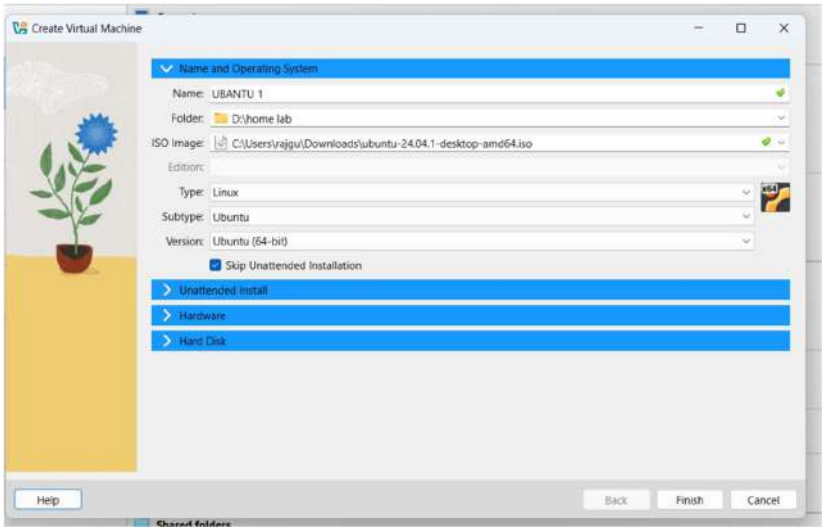
The ISO is ~5GB.

After the download is complete you will have a **.iso** file.

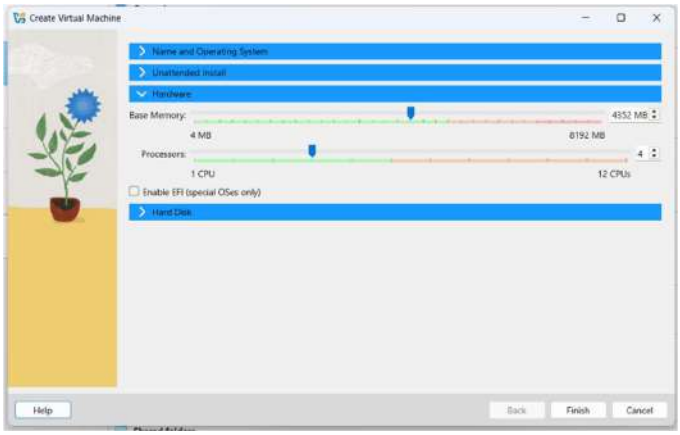
In VirtualBox from the sidebar select **Tools** and then click on **New** from the toolbar.



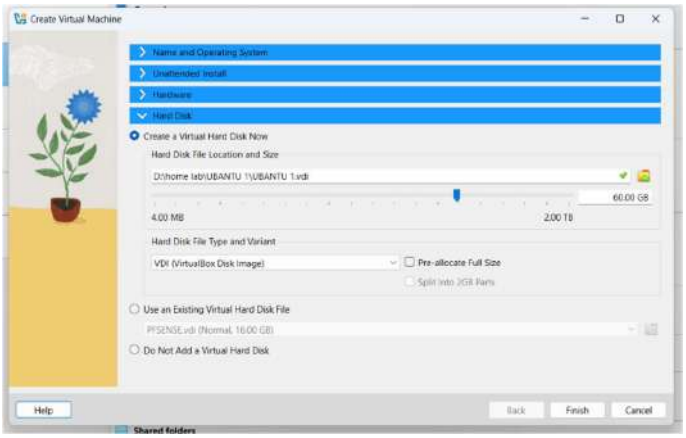
Give the VM a name. Select the downloaded ISO image. Select the "Skip Unattended Installation" option and click on **Next**.



Increase the Base Memory to **4096MB** (4GB) and click on **Next**.

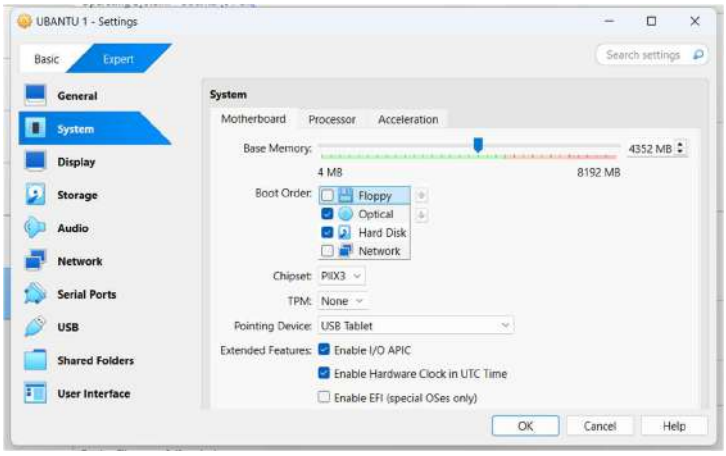


Increase the Hard Disk size to **60GB** and click on **Finish**.

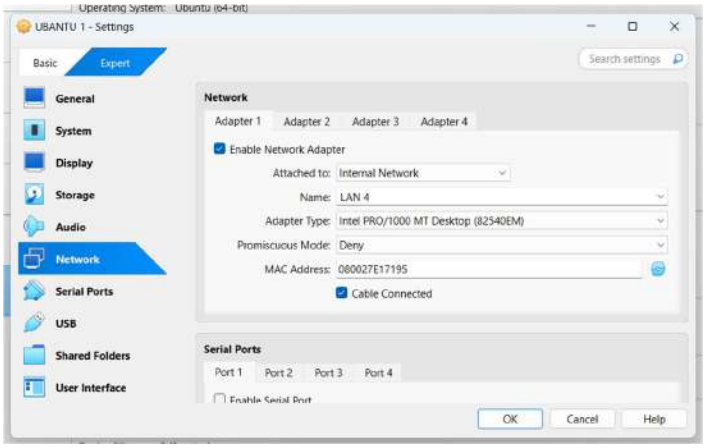


Select the VM and click on **Settings** from the toolbar.

Go to **System -> Motherboard**. In Boot Order ensure that **Hard Disk** is on the top followed by **Optical**. Uncheck **Floppy**.

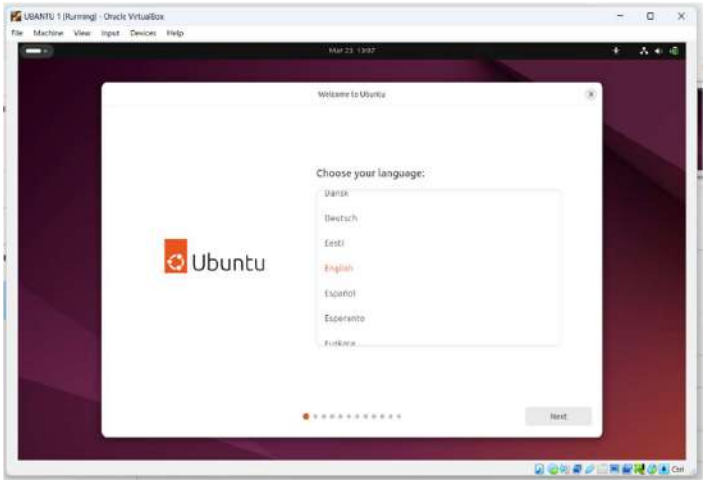


Go to **Network -> Adapter 1**. For the Attached to field select **Internal Network**.
For name select **LAN 4**. Click on **OK** to save changes.

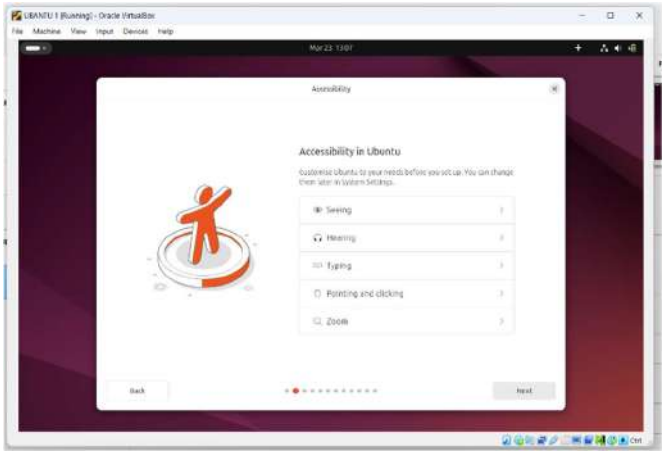


Select the VM and click on **Start**.

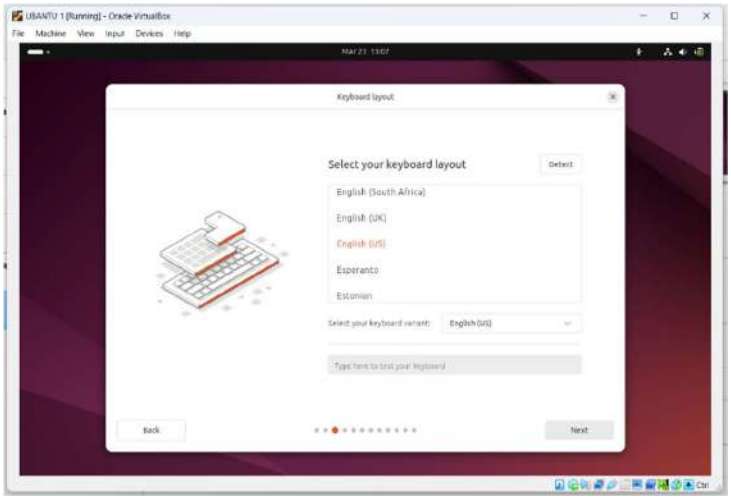
Then Click **Next.**



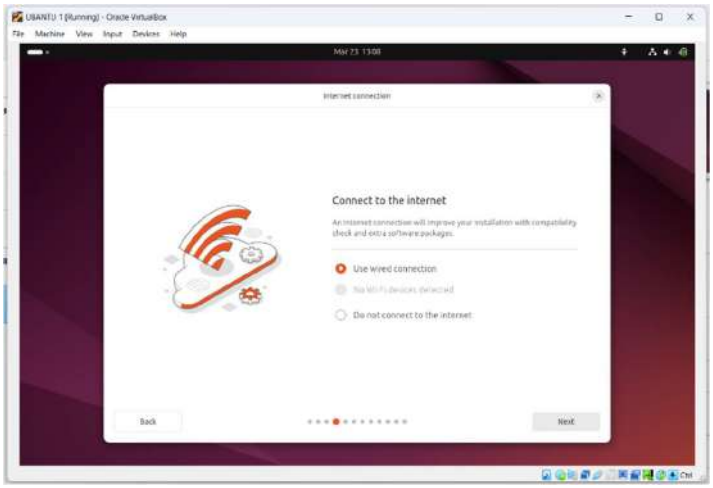
Then Click **Next.**



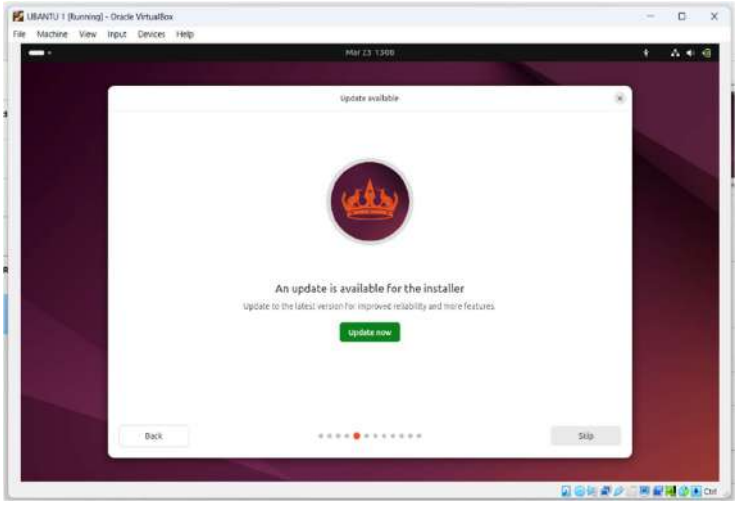
Then Click **Next.**



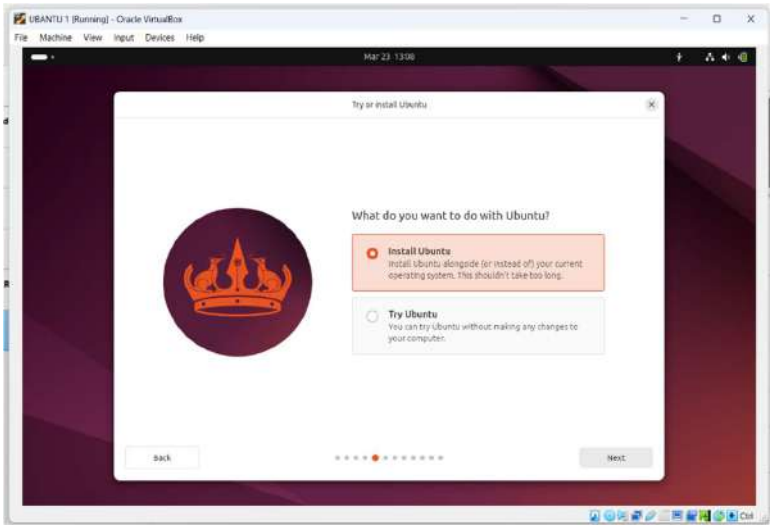
Then Click **Next.**



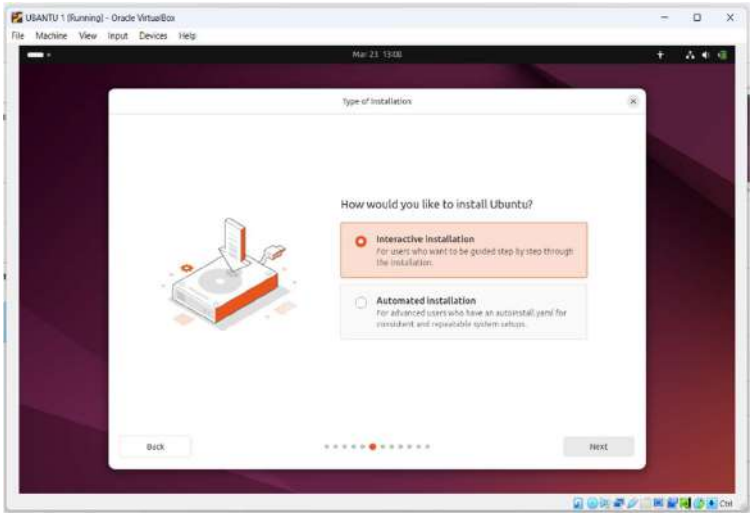
Then Click **Skip.**



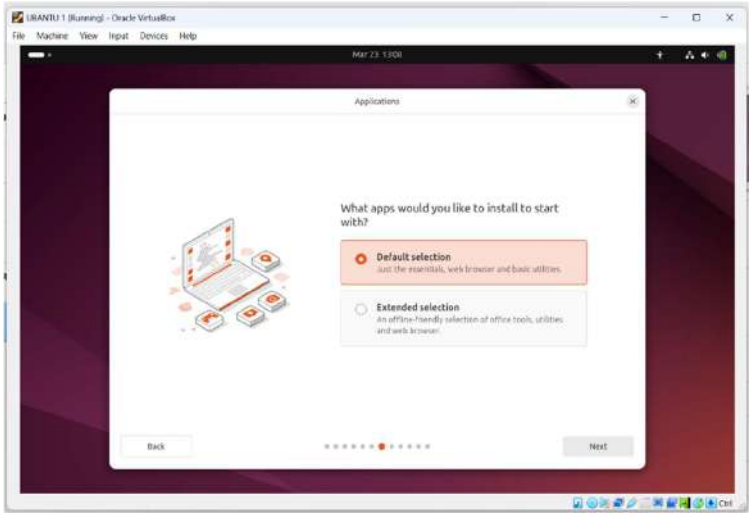
Then Click **Next.**



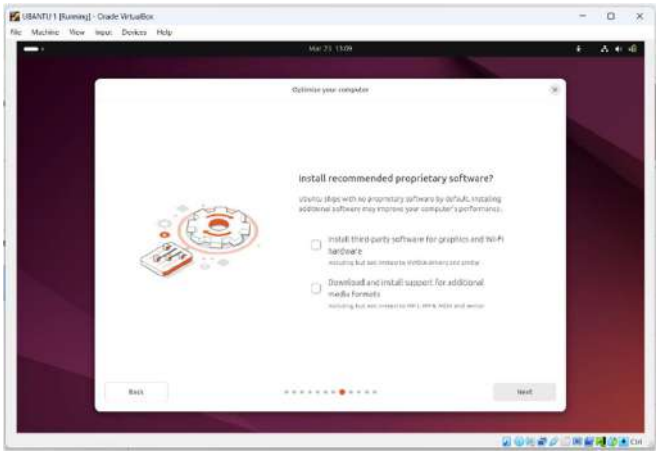
Then Click **Next.**



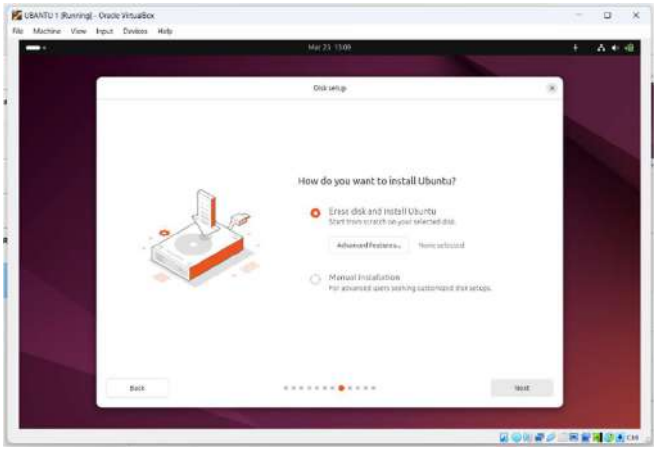
Then Click **Next.**



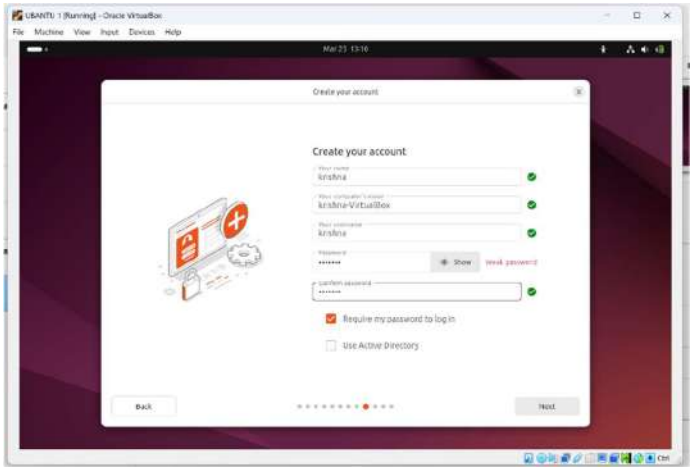
Then Click **Next.**



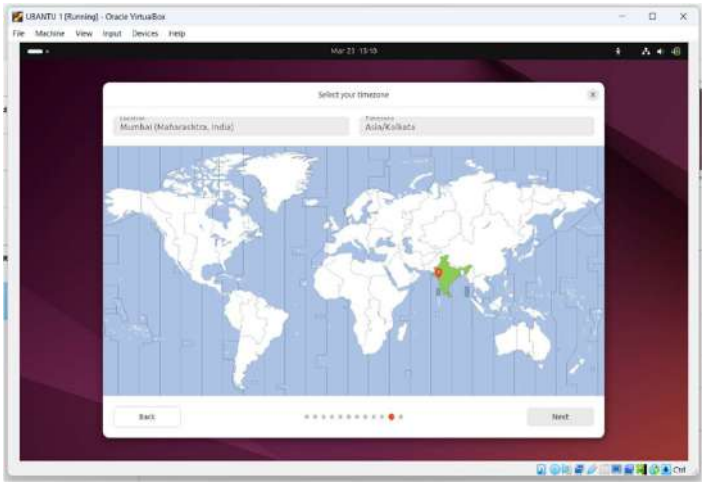
Then Click **Next.**



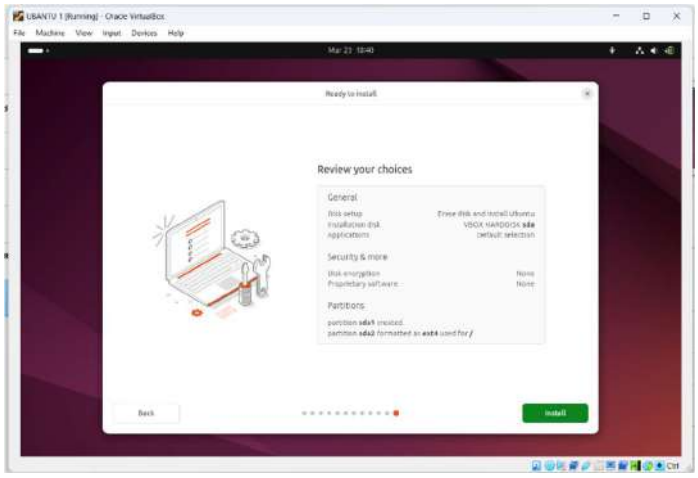
Enter the username, password and hostname and click on **Next.**



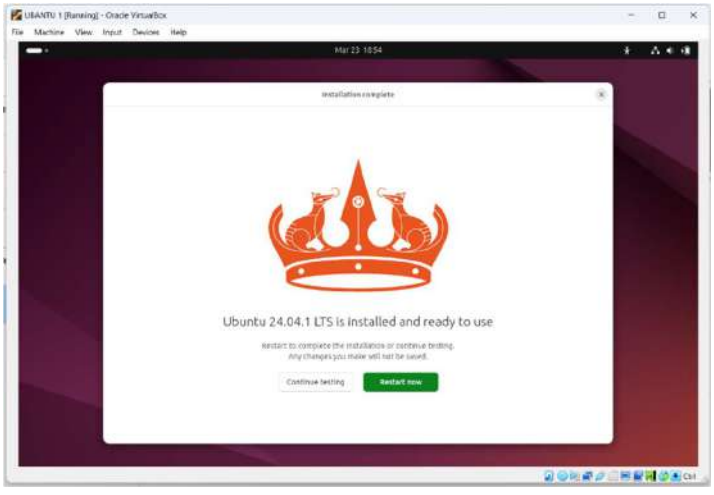
Then Click **Next.**



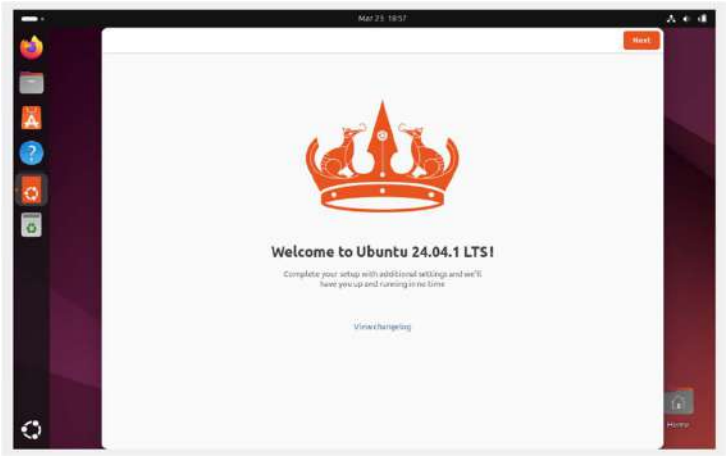
Then Click **Install.**



After Installation click on **Restart.**

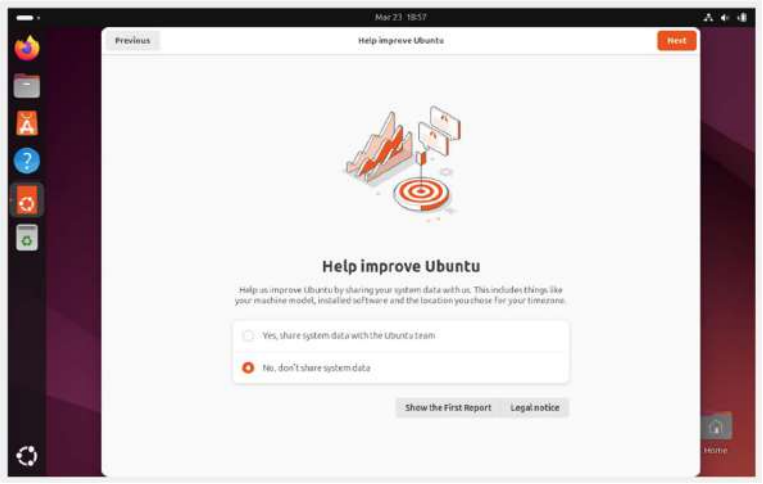


Then Click **Next.**

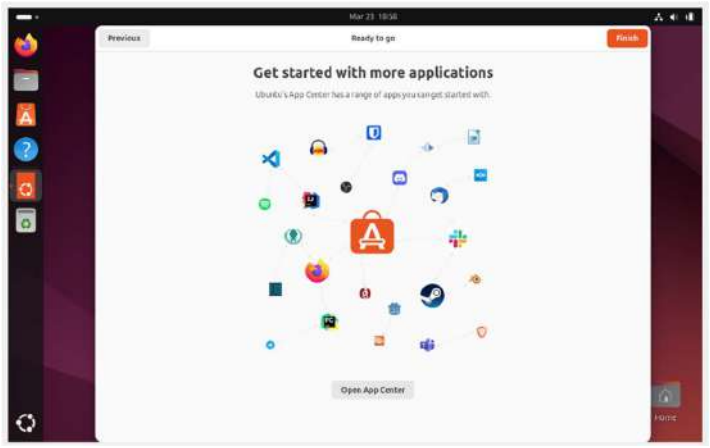


Click **Next.**

Select "No, don't send system info" and click on **Next**.

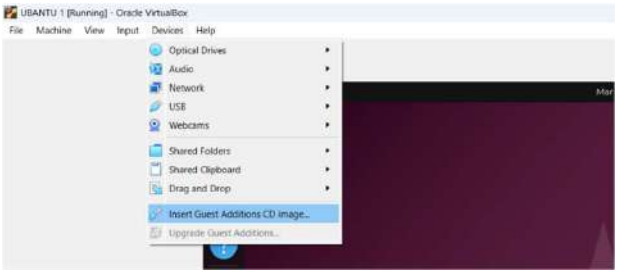


Click on **Finish.**



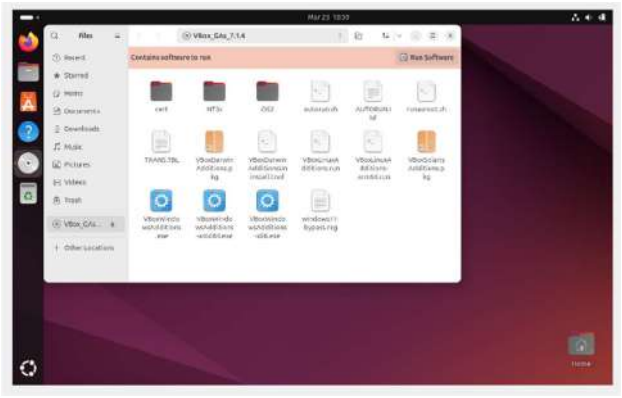
Install Guest Additions

From the VM toolbar select **Devices -> Install Guest Additions CD image**.



The disk will show up on the dock. Click on it to view the content of the disk.

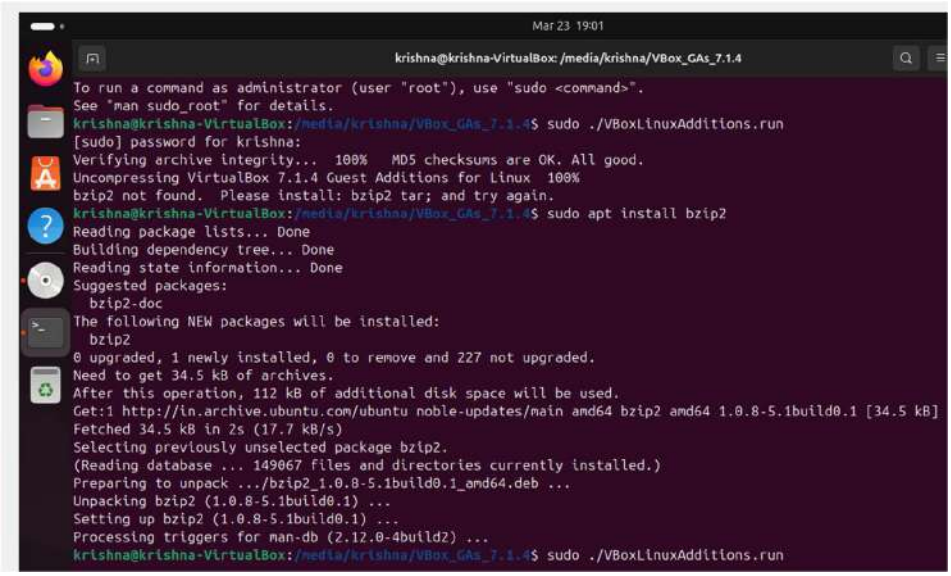
Right-click anywhere in the empty area in the File Explorer and select "Open in Terminal".



Run the following command to install Guest Additions:

sudo ./VBoxLinuxAdditions.run

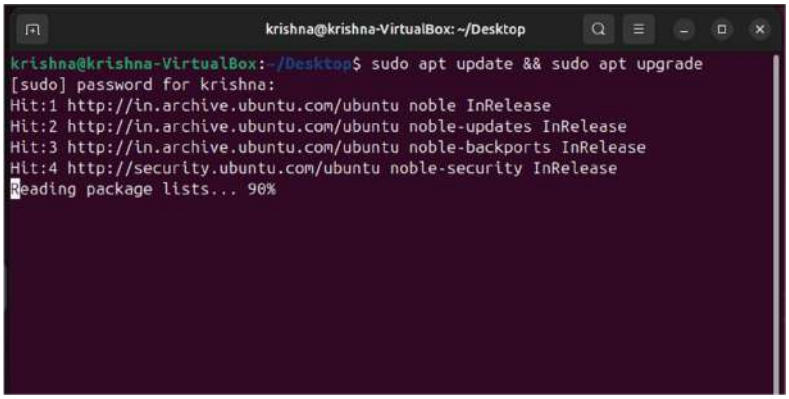
before this installation run **sudo apt install bzip2** because it needs for installation



Once the installation is complete close the terminal, right-click on the disk icon in the dock and select **Eject**.

Press **Ctrl+Alt+T** to open a new terminal then enter the following command to update the system:

sudo apt update && sudo apt full-upgrade



use the following link to directly download Splunk v9.1.2:
Splunk Enterprise 9.1.2 - Linux (.deb) - Direct Download Link

Once the download is complete we will have a **.deb** file. Open the Terminal (**Ctrl+Alt+t**) and navigate to the Downloads folder.

cd Downloads

Run the following following command to install curl (dependency for Splunk):

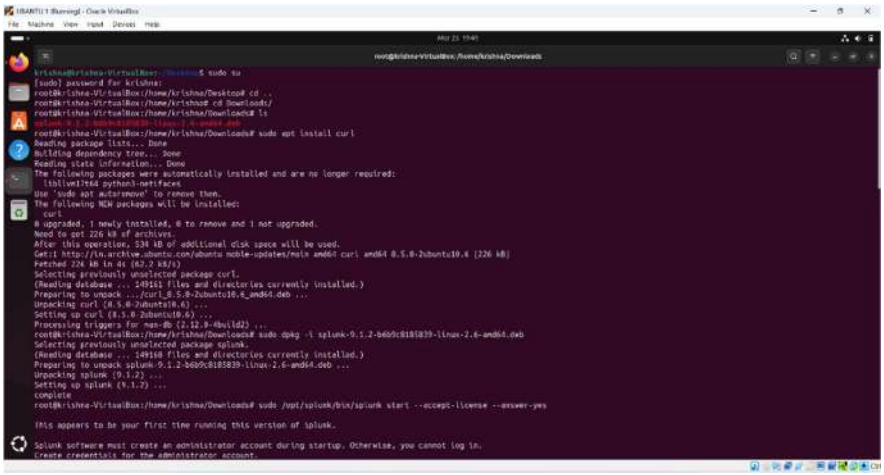
sudo apt install curl

Run the following command to install Splunk:

sudo dpkg -i splunk-9.1.2-b6b9c8185839-linux-2.6-amd64.deb

After the installation is completed use the following command to launch Splunk:

sudo /opt/splunk/bin/splunk start --accept-license --answer-yes



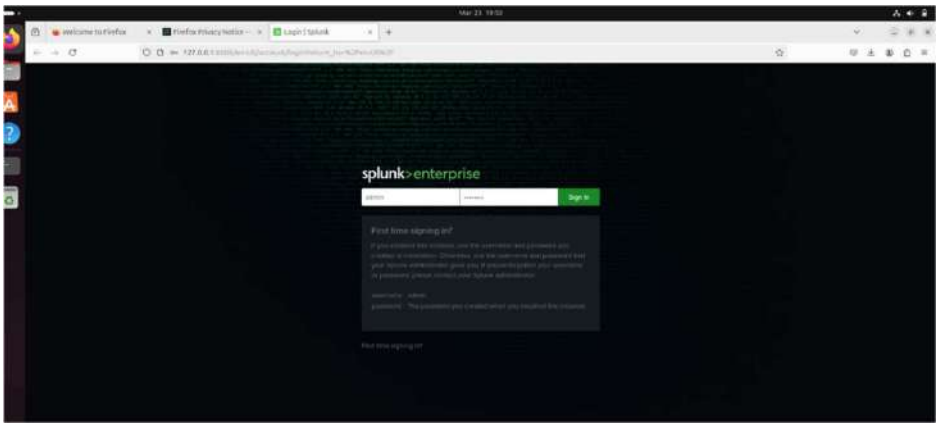
Provide a name and password when prompted. These credentials need to be used to log into Splunk.

Once the setup is complete we see the Splunk is running on **http://127.0.0.1:8000**

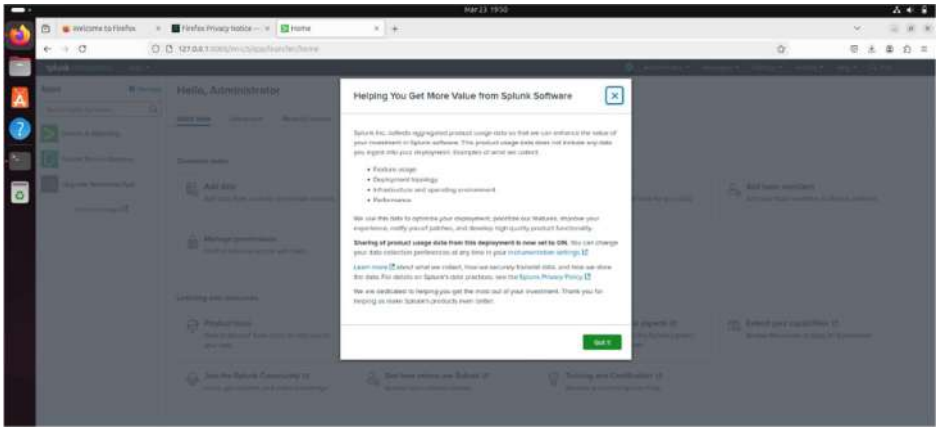
Run the following to allow Splunk to start automatically when the system is booted.

sudo /opt/splunk/bin/splunk enable boot-start

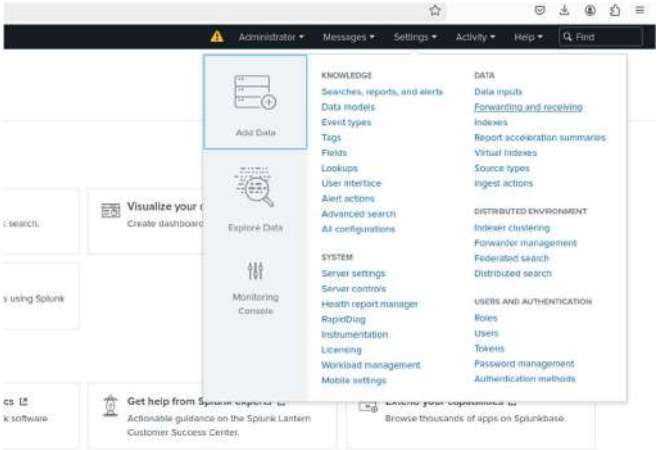
Before we can install Splunk Universal Forwarder there are a few settings we need to change in Splunk. Open Splunk by going to **http://127.0.0.1:8000**.



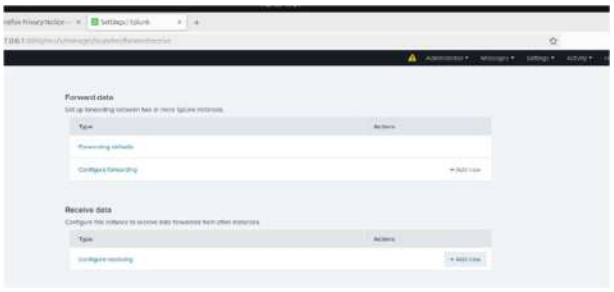
Click on **got it**.



From the toolbar select **Settings -> Forwarding and receiving**.



Click on "Add new" in the Receive data section.



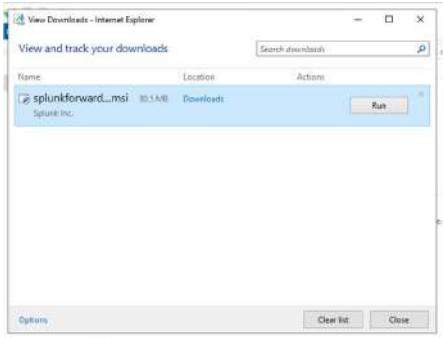
Enter **9997** as the port to listen for incoming data. Click on **Save**.

The next steps need to be performed on the Domain Controller (Windows Server 2019). We are going to ingest the log data that is generated by this device into Splunk.

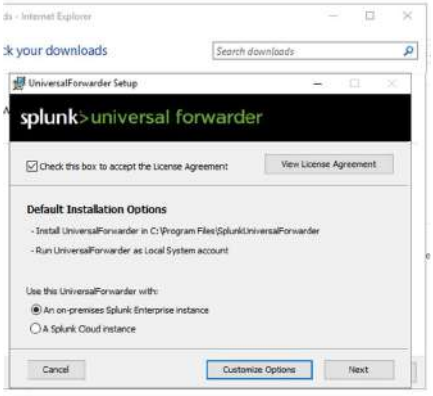
Go to the following link to download Universal Forwarder: Download Universal Forwarder for Remote Data Collection | Splunk

You need to log in to be able to download the setup. Select the Windows tab and then click on the Download Now button beside the 64-bit option.

Run the **.msi** file to begin installation.



Check the box on the top to accept the agreement and then click on **Next**.



Provide a username and password for the Forwarder. I would recommend using the same credentials that were configured on Splunk.

For the new step need the IP address of the Ubuntu (Splunk) VM. Use the following command to get the IP address.

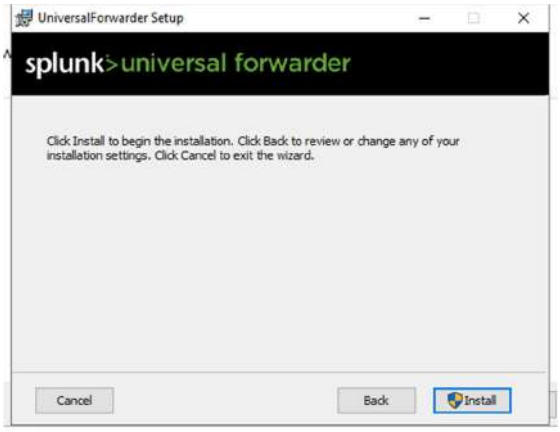
ip a

```
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
root@krishna-VirtualBox:/home/krishna/Downloads# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e1:71:95 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.11/24 brd 10.10.10.255 scope global dynamic noprefixroute enp0s3
       valid_lft 6680sec preferred_lft 6680sec
    inet6 fe80::a00:27ff:fee1:7195/64 scope link
       valid_lft forever preferred_lft forever
root@krishna-VirtualBox:/home/krishna/Downloads#
```

Enter the IP address of the Splunk VM (in my case **10.10.10.13**) and enter **8089** as the value for the port field then click on **Next**.

Again enter the Splunk VM IP address and for port enter **9997**. This is the port we configured in Splunk. Click on **Next** to continue.

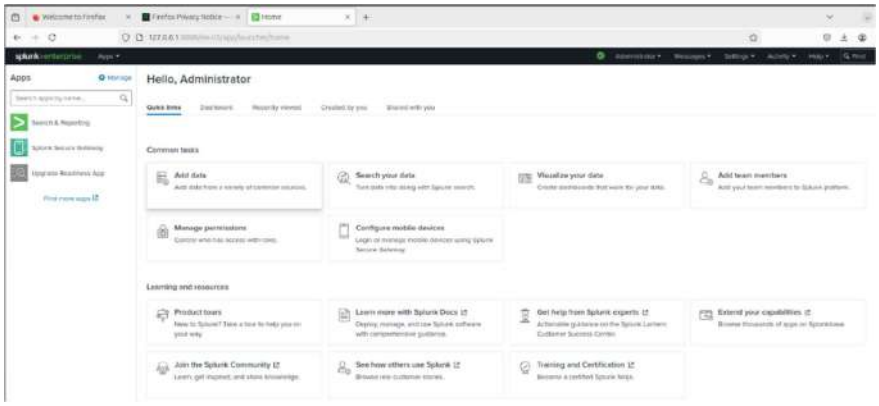
Click on **Install**.



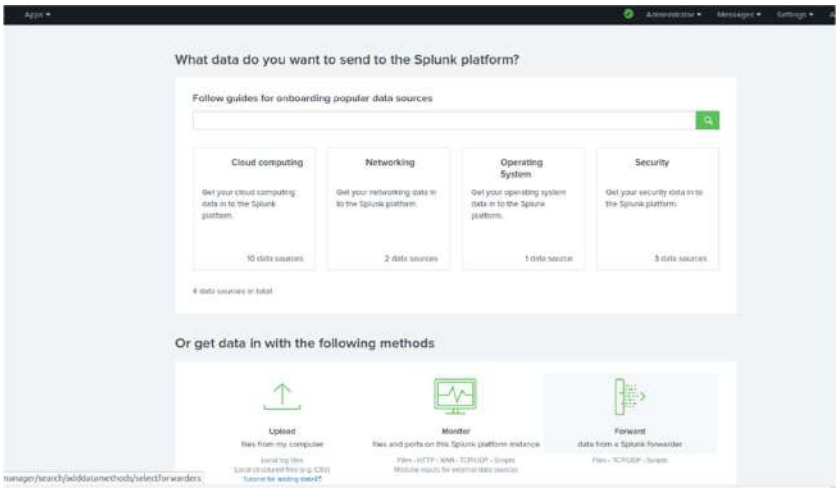
Click on **Finish** to close the installer.

Now that we have Splunk and Universal Forwarder configured we need to link both the pieces together so that Splunk can collect data.

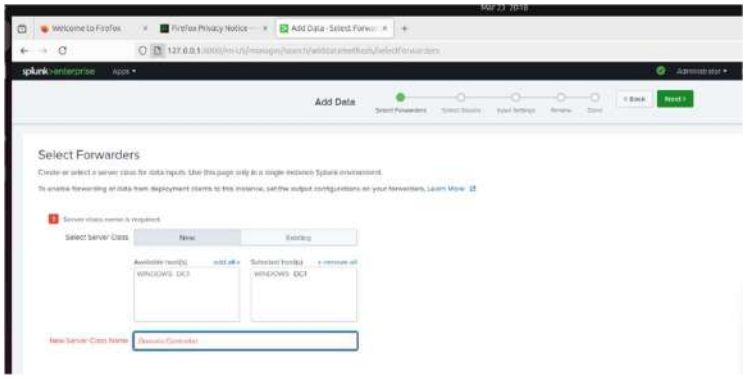
In Splunk select **Settings -> Add Data**.



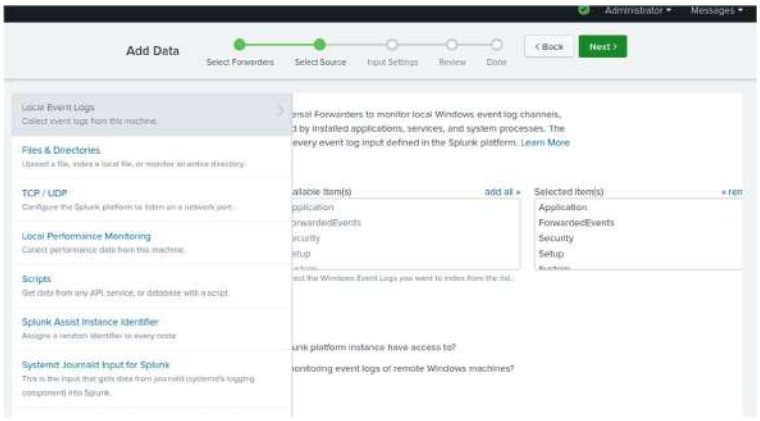
Click on **Forward**.



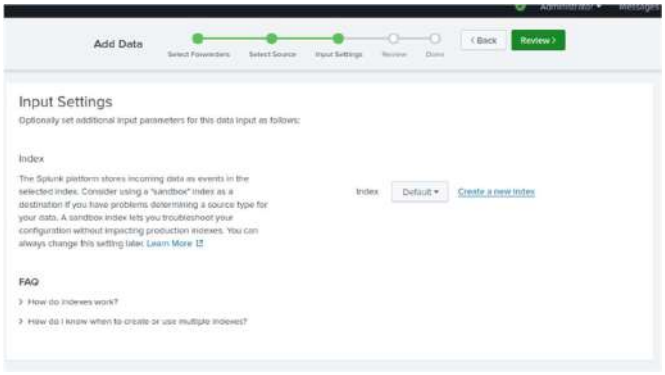
Our DC VM should automatically show up in the left box. Click on "add all" to move it to the right side. In the "New Source Class Name" field provide a name for the source. Click on **Next** to continue.



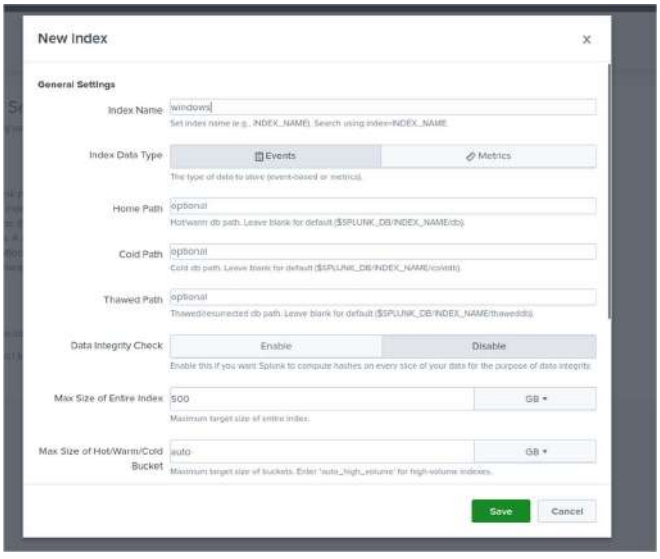
Select "Local Event Logs" then click on the "add all" button above the dropdown field to ingest all the logs generated by the DC. Click on **Next** once done.



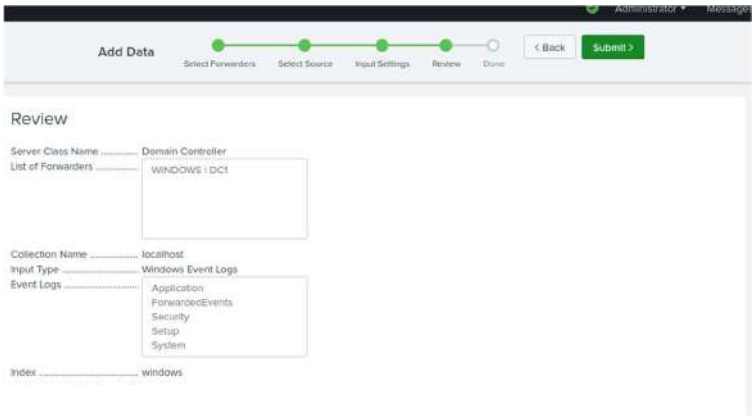
Click on "Create a new index".Indexes are the Splunk equivalent of SQL Tables. It is used to store similar data.



Provide the Index a name. Keep all the other fields on their default value and click on **Save** then click on **Next**.

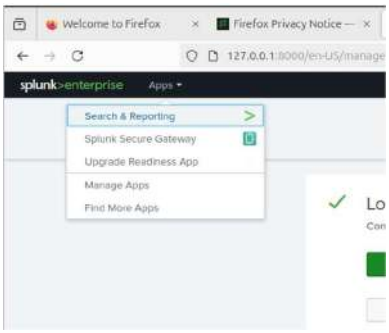


Confirm all the options look correct and click on **Submit**.



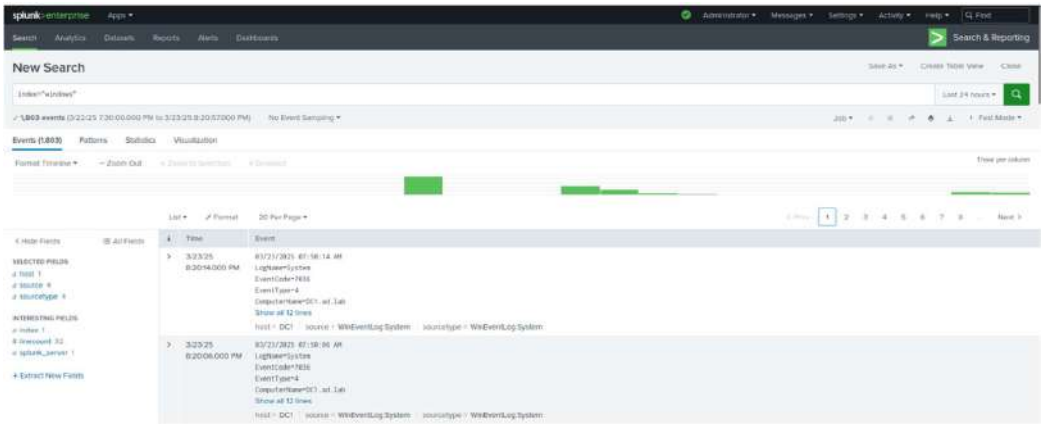
Querying Data

From the Splunk toolbar select **Apps -> Search & Reporting**.



In the search box enter the following to view the ingested data:

In the above command “windows” is the name I gave my index



Conclusion : I have successfully completed Home Lab Security for my Digital forensics Project.