

## **OVERVIEW OF VIRTUAL SECURITY HOME LAB**

This home lab is created for homelab security understanding 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,ubuntu,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 :

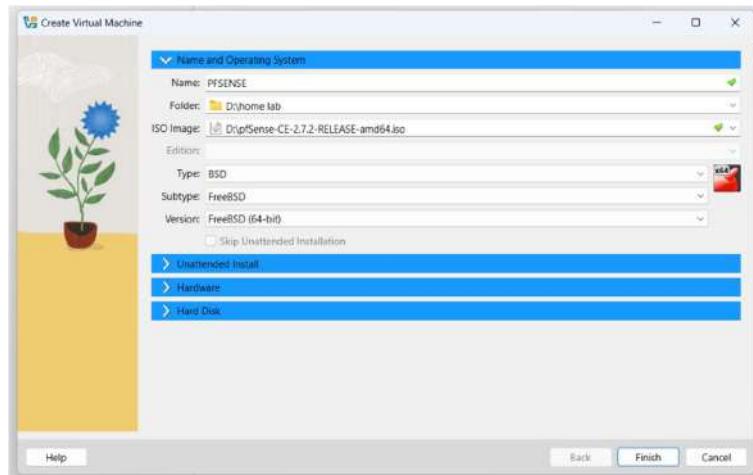
<https://atxfiles.netgate.com/mirror/downloads/pfSense-CE-2.7.2-RELEASE-amd64.iso.gz>

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

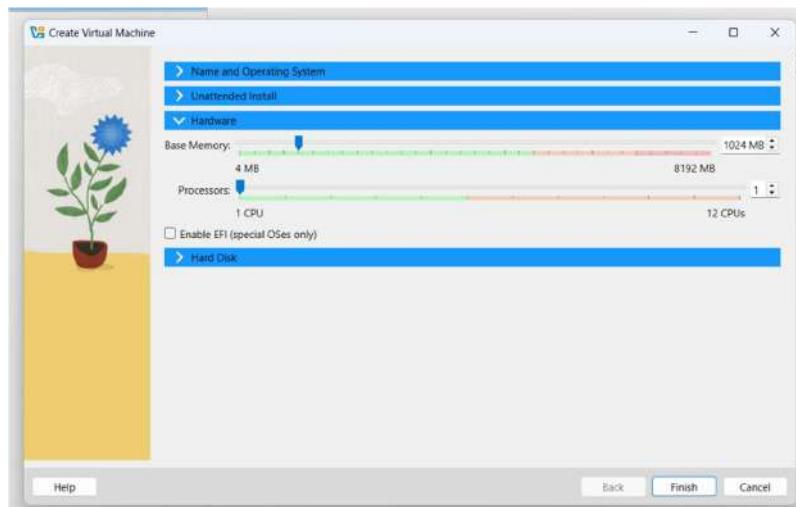
After extracting, you'll get a **.iso** file.

Open VirtualBox → Click Tools → Click New.

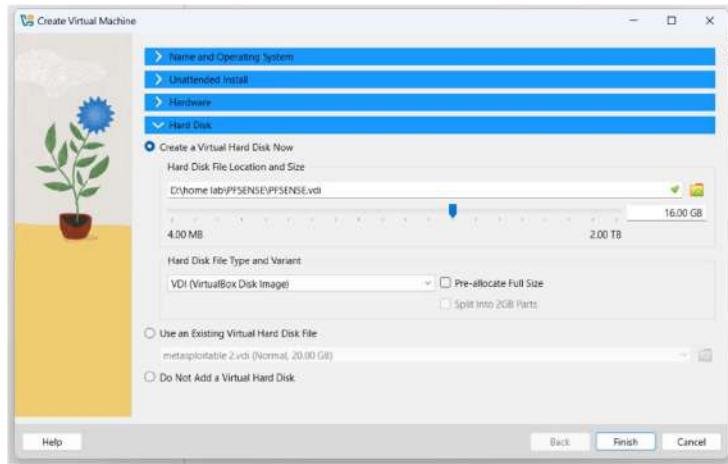
Enter a **name**, choose a **folder**, select **ISO Image** → **Others** → **your .iso file**, set **Type: BSD**, **Version: FreeBSD (64-bit)**, then click **Next**. 



Click next

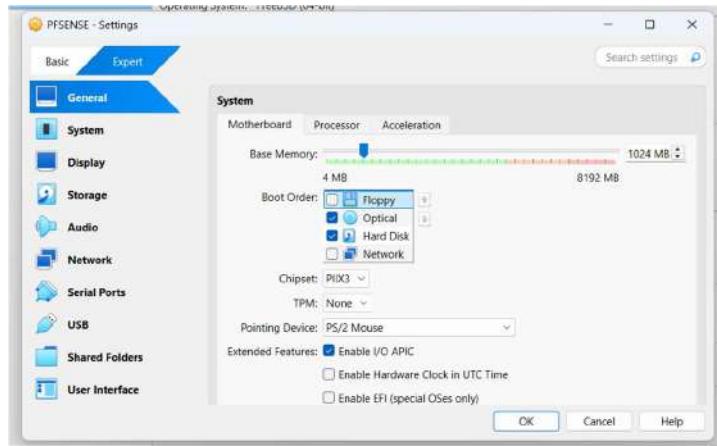


Click finish



Click on settings after virtual machine added

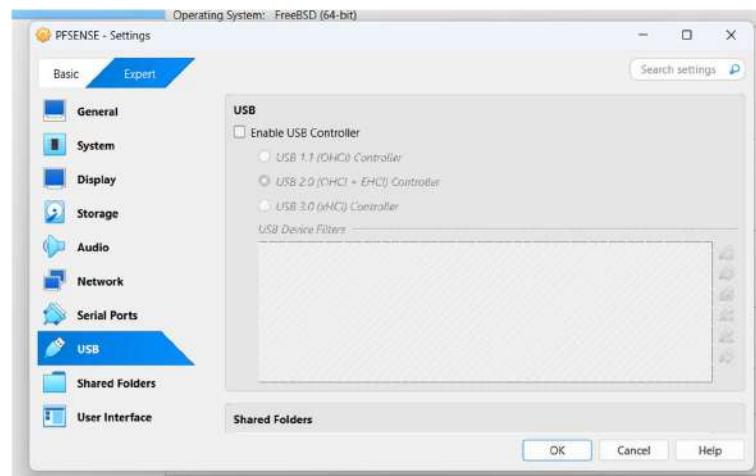
Then click system option after clicking system option then untick floppy disk



Then click Audio and untick it

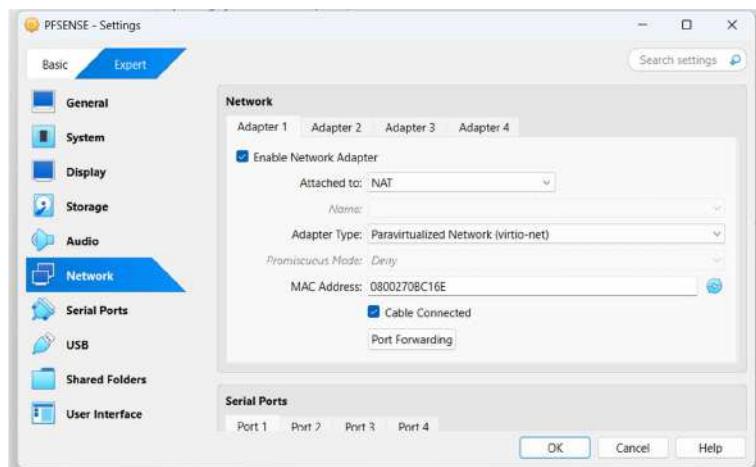


After we have to untick USB also

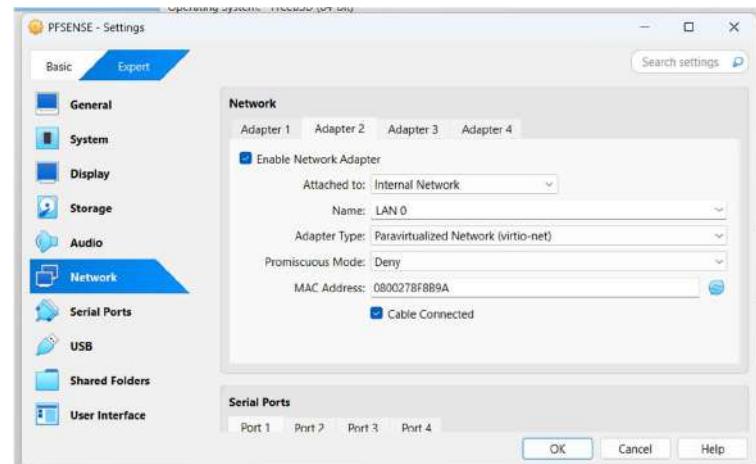


In last we are adding networks

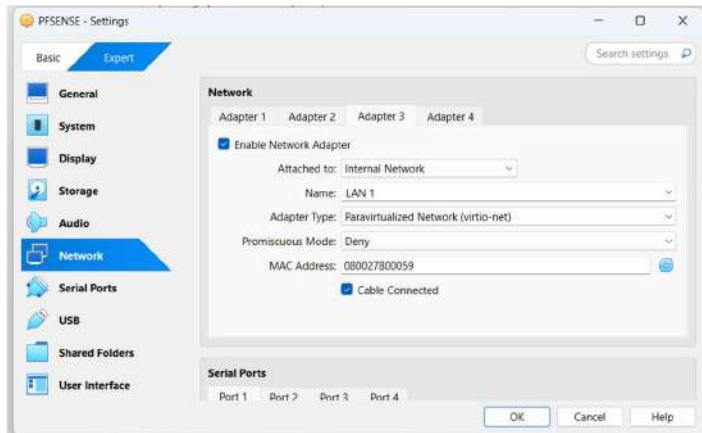
**Network → Adapter 1 → Set Attached to: NAT → Expand Advanced → Set Adapter Type: Paravirtualized Network (virtio-net).**



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

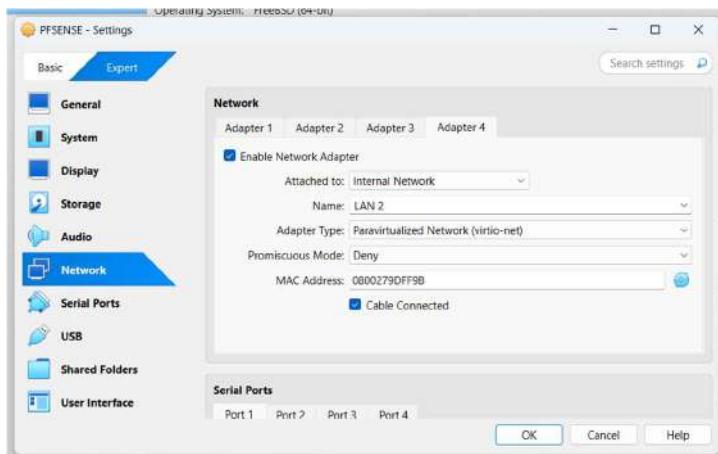


**Adapter 3 → Enable Network Adapter → Set Attached to: Internal Network → Name: LAN 1 → Expand Advanced → Set Adapter Type: Paravirtualized Network (virtio-net).**



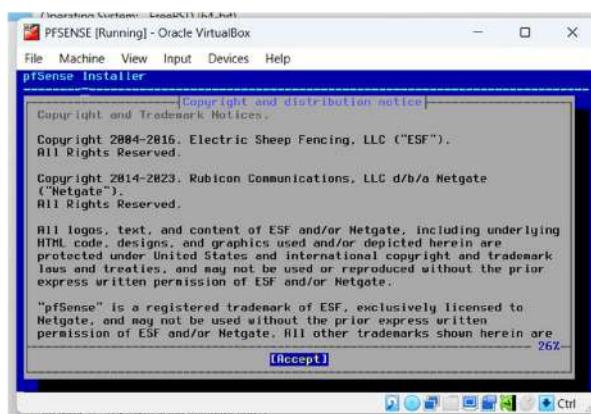
**Adapter 4 → Enable Network Adapter → Set Attached to: Internal Network → Name: LAN 2 → Expand Advanced → Set Adapter Type: Paravirtualized Network (virtio-net).**

Click **OK** to save and exit.

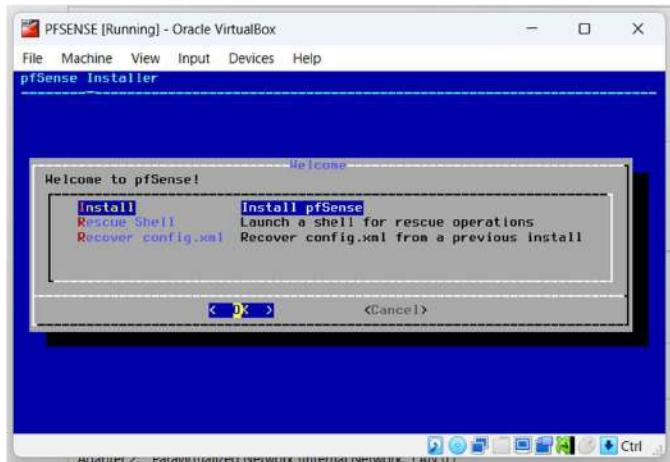


Select the pfSense VM from the sidebar and click on **Start** from the toolbar.

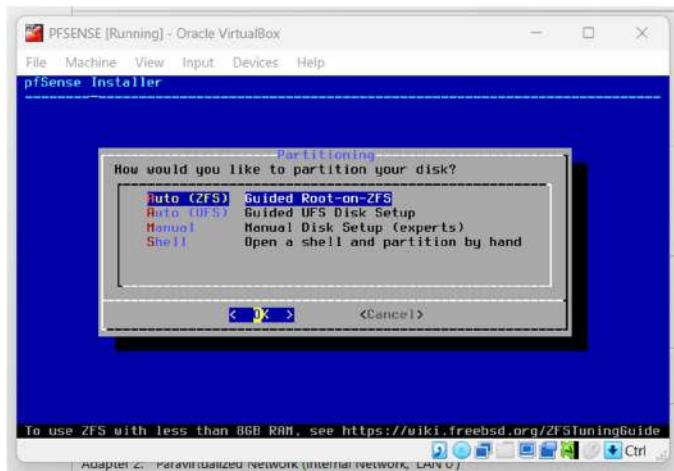
Wait for the text to finish loading, then press **Enter** to accept the agreement.



Press **Enter** to start the Installation.

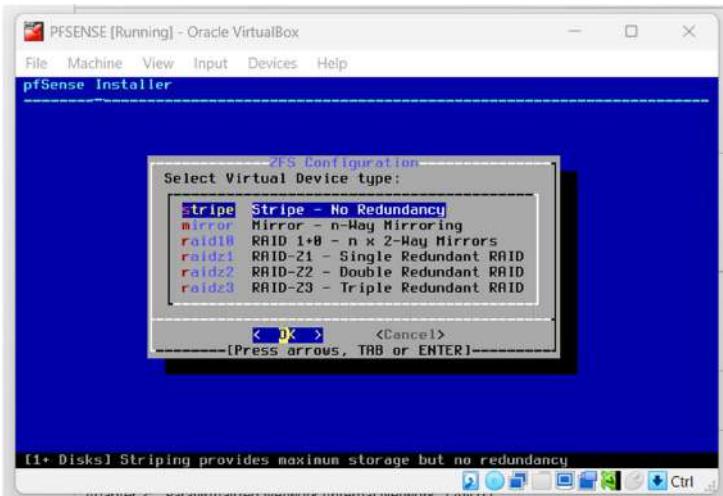


Press **Enter** to select the Auto (ZFS) partition option.

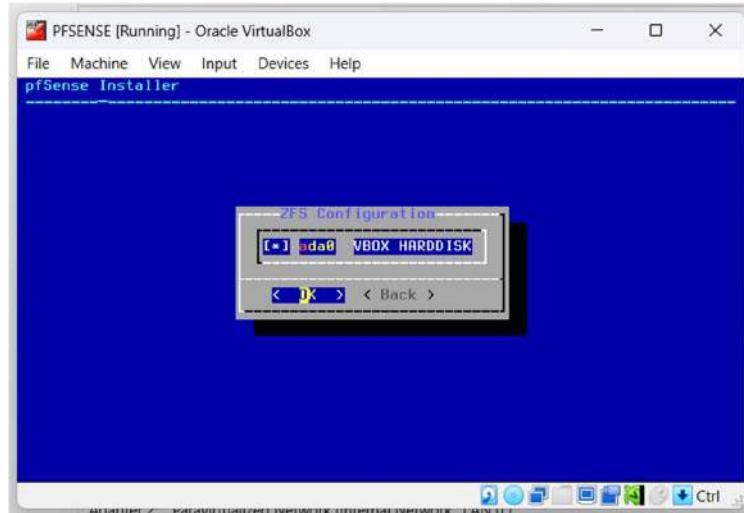


Press **Enter** to select Proceed with Installation.

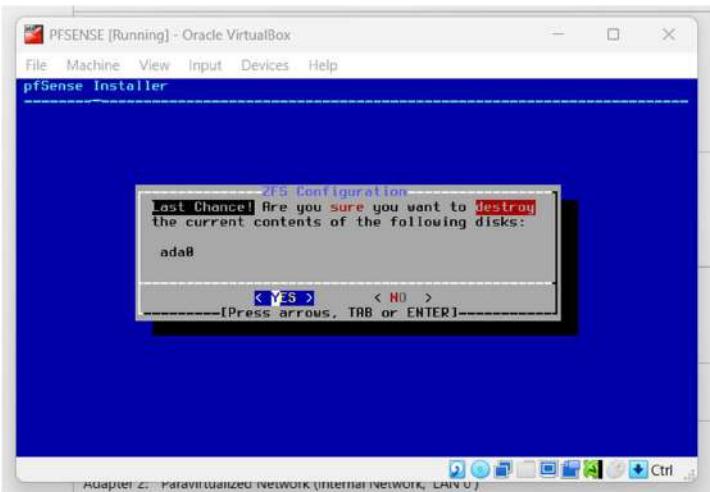
Press **Enter** to select Stripe - No Redundancy.



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

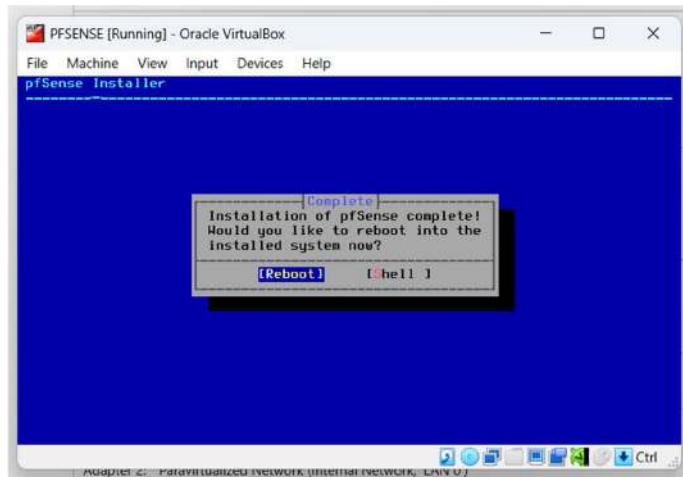


Use the Left Arrow to select **YES** and then press **Enter** to continue.



Wait for the installation to complete.

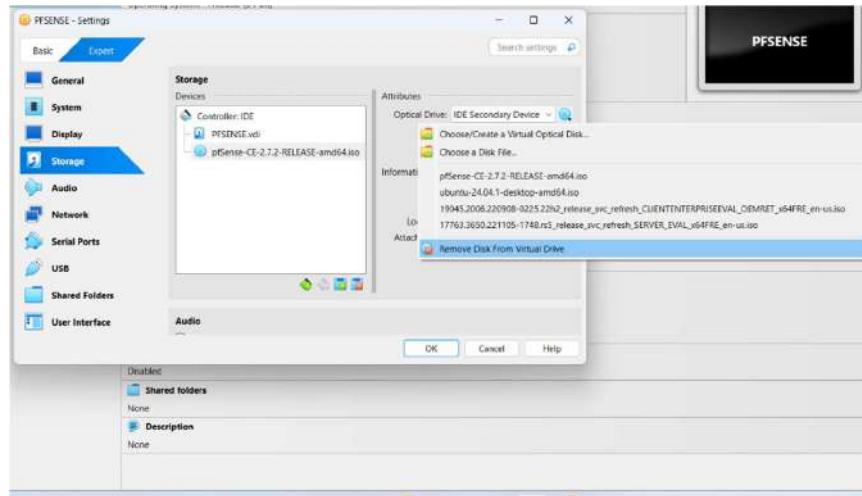
Press **Enter** to Reboot the VM.



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.

```
Vtnet0: link state changed to UP
Vtnet1: link state changed to UP
Vtnet2: link state changed to UP
Vtnet3: link state changed to UP

Valid interfaces are:
Vtnet0 00:00:27:0b:c1:6e (down) VirtIO Networking Adapter
Vtnet1 00:00:27:0f:0b:9a (down) VirtIO Networking Adapter
Vtnet2 00:00:27:00:00:59 (down) VirtIO Networking Adapter
Vtnet3 00:00:27:9d:ff:9b (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]? 2025-03-22T09:30:07.364616+00:00 - php-fpm 394
- /rc.linkup: Ignoring link event during boot sequence.
2025-03-22T09:30:07.466608+00:00 - php-fpm 394 - - /rc.linkup: Ignoring link eve
nt during boot sequence.
2025-03-22T09:30:07.470282+00:00 - php-fpm 394 - - /rc.linkup: Ignoring link eve
nt during boot sequence.
2025-03-22T09:30:07.537357+00:00 - php-fpm 394 - - /rc.linkup: Ignoring link eve
nt during boot sequence.
```

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**

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

Enter the WAN interface name or 'a' for auto-detection
(vtnet0 vtnet1 vtnet2 vtnet3 or a): vtnet0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet1 vtnet2 vtnet3 a or nothing if finished): vtnet1

Enter the Optional 1 interface name or 'a' for auto-detection
(vtnet2 vtnet3 a or nothing if finished): vtnet2

Enter the Optional 2 interface name or 'a' for auto-detection
(vtnet3 a or nothing if finished): vtnet3

The interfaces will be assigned as follows:
WAN -> vtnet0
LAN -> vtnet1
OPT1 -> vtnet2
OPT2 -> vtnet3

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

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

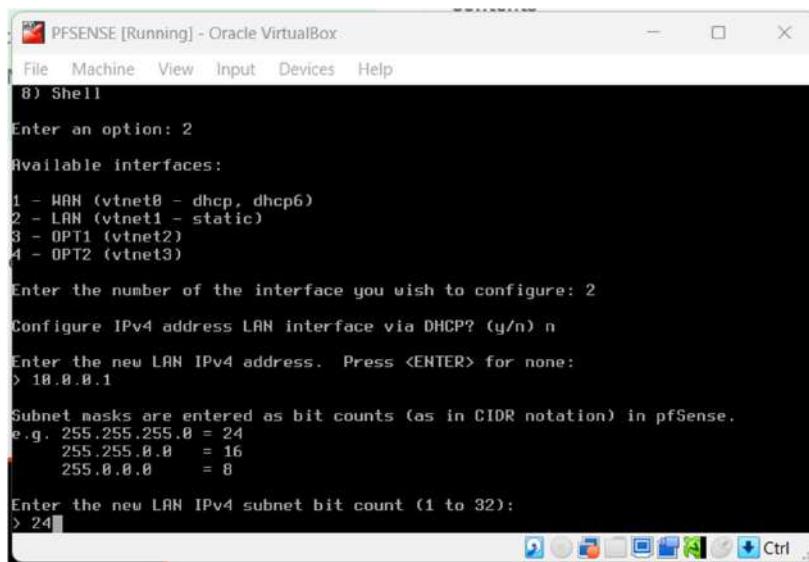
### Configuring LAN (vtnet1)

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.

```

PFSENSE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
>
Configure IPv6 address L2N interface via DHCP6? (y/n) n
Enter the new L2N IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on L2N? (y/n) y
Enter the start address of the IPv4 client address range: 10.8.0.11
Enter the end address of the IPv4 client address range: 10.8.0.243
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
Please wait while the changes are saved to L2N...
Reloading filter...
Reloading routing configuration...
DHCPD...
The IPv4 L2N address has been set to 10.8.0.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
https://10.8.0.1/
Press <ENTER> to continue.

```

## 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**

```

PFSENSE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
③ Shell
Enter an option: 2
Available interfaces:
1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)
3 - OPT1 (vtnet2)
4 - OPT2 (vtnet3)
Enter the number of the interface you wish to configure: 3
Configure IPv4 address OPT1 interface via DHCP? (y/n) n
Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 10.6.6.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0 = 16
      255.0.0.0 = 8
Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 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**

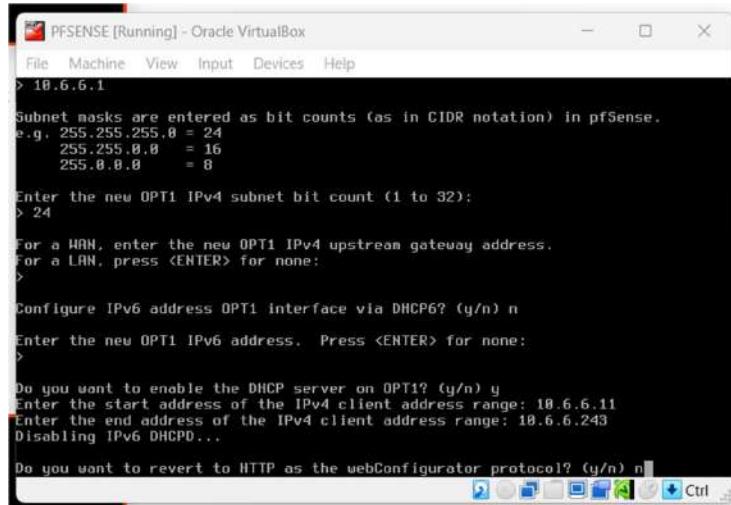
For the new OPT1 IPv6 address question press **Enter**

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**



```

PFSENSE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
> 10.6.6.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.8 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8
Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 24
For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Configure IPv6 address OPT1 interface via DHCP6? (y/n) n
Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on OPT1? (y/n) 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
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

```

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

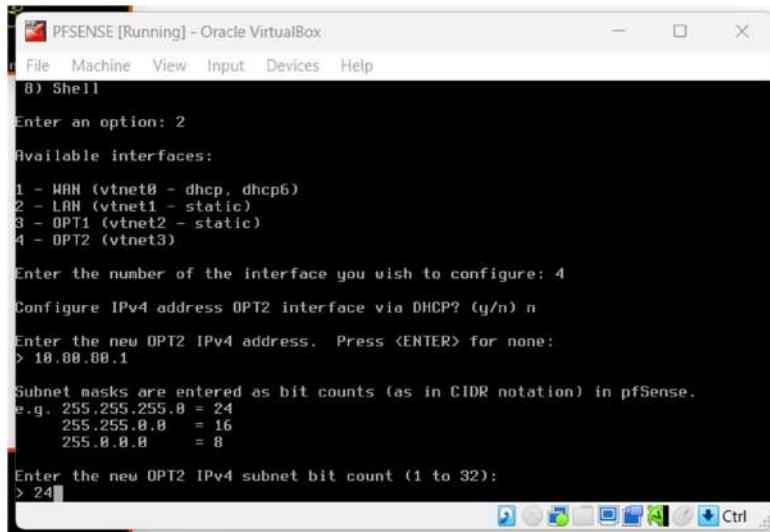
### Configuring OPT2 (vtnet3)

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**



```

PFSENSE [Running] - Oracle VirtualBox
File Machine View Input Devices Help
0) Shell
Enter an option: 2
Available interfaces:
1 - WAN (vtnet0 - dhcp, dhcp6)
2 - LAN (vtnet1 - static)
3 - OPT1 (vtnet2 - static)
4 - OPT2 (vtnet3)

Enter the number of the interface you wish to configure: 4
Configure IPv4 address OPT2 interface via DHCP? (y/n) n
Enter the new OPT2 IPv4 address. Press <ENTER> for none:
> 10.80.80.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.8 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8
Enter the new OPT2 IPv4 subnet bit count (1 to 32):
> 24

```

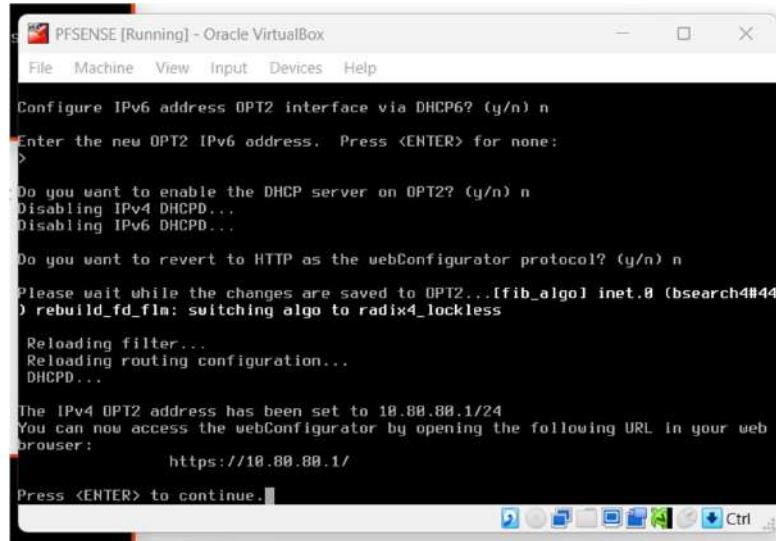
For the next question directly press **Enter**. Since **OPT2** is a **LAN** interface we do not have to worry about configuring the upstream gateway.

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**



```
Configure IPv6 address OPT2 interface via DHCP6? (y/n) n
Enter the new OPT2 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT2? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

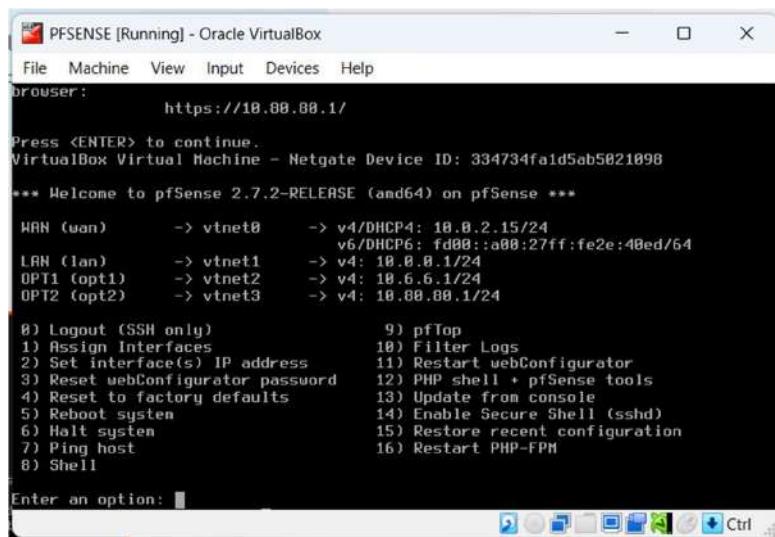
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
Please wait while the changes are saved to OPT2...[fib_algo] inet.0 (bsearch4#44
) rebuild_fd_fln: switching algo to radix4_lockless

Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 OPT2 address has been set to 10.80.80.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
https://10.80.80.1/
Press <ENTER> to continue.
```

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:



```
File Machine View Input Devices Help
browser:
https://10.80.80.1/
Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 334734fa1d5ab5021098
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> vtnet8      -> v4/DHCP4: 10.8.2.15/24
                  v6/DHCP6: fd00:a00:27ff:fe2e:40ed/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)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM

Enter an option: 6
```

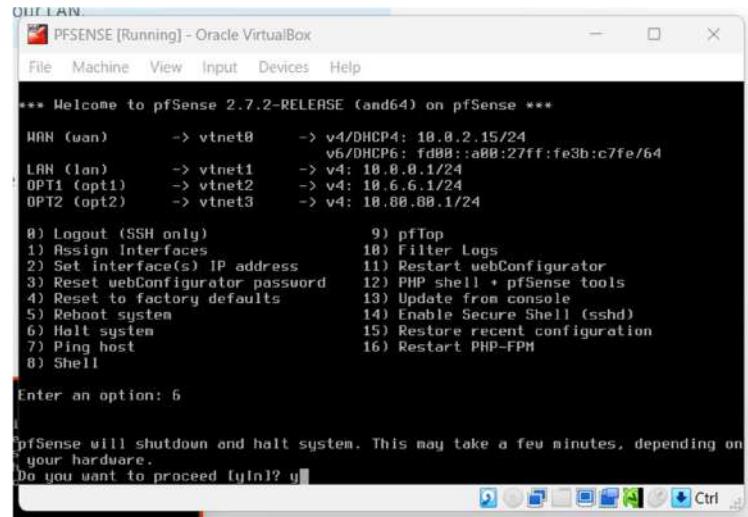
Interface setup in **pfSense** is complete.

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.



## 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

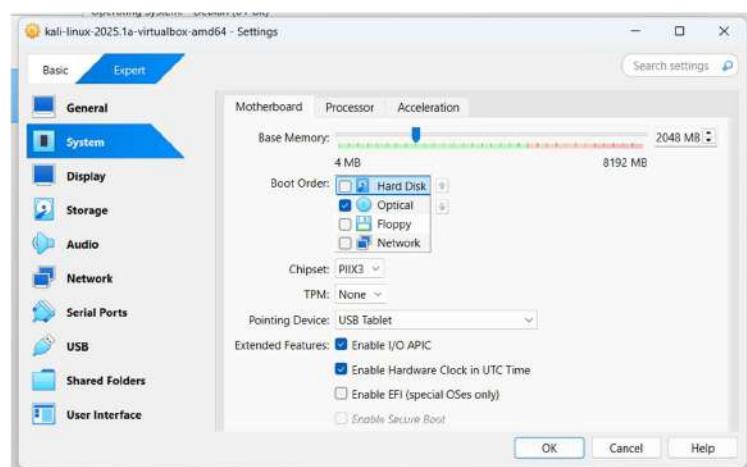
After installation unzip kali virtual box machine

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

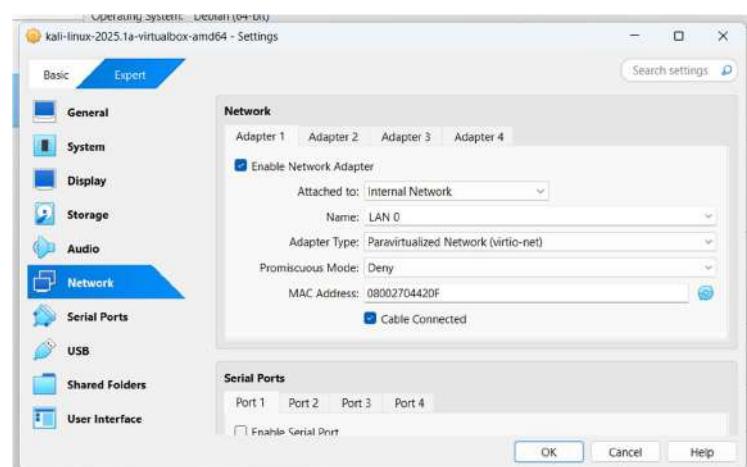
Go to **System -> Motherboard**. For the Boot Order option ensure that the **Hard Disk** is on the top followed by **Optical**. Uncheck **Floppy**.



### 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)**.

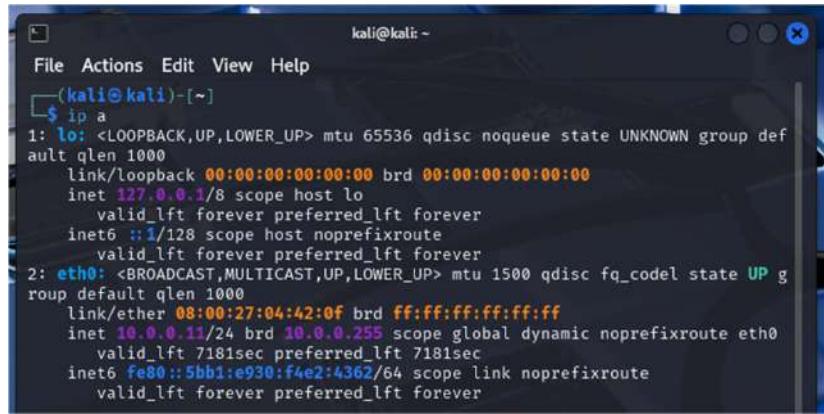


Then start kali machine

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.

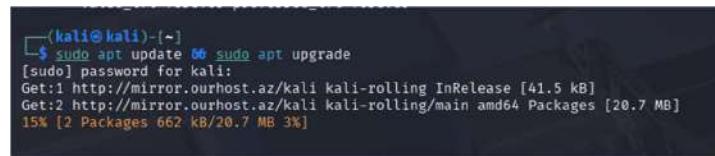


```
kali㉿kali:~
File Actions Edit View Help
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.11/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
        valid_lft 7181sec preferred_lft 7181sec
    inet6 fe80::5bb1:e930:f4e2:4362/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Use the following command to update the system:

**Sudo apt update && sudo apt get update**

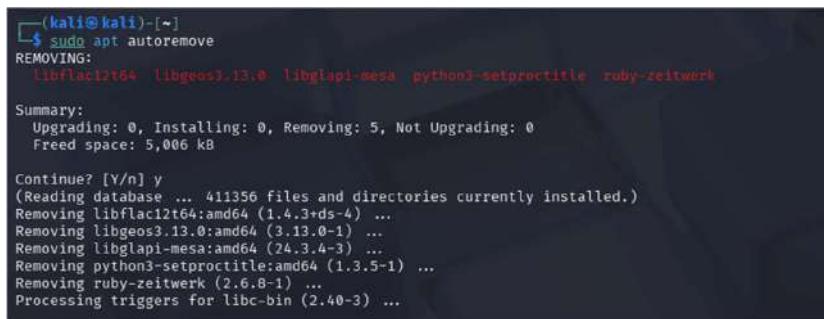
Enter password when prompted.



```
(kali㉿kali)-[~]
$ sudo apt update && sudo apt upgrade
[sudo] password for kali:
Get:1 http://mirror.ourhost.az/kali kali-rolling InRelease [41.5 kB]
Get:2 http://mirror.ourhost.az/kali kali-rolling/main amd64 Packages [20.7 MB]
15% [2 Packages 662 kB/20.7 MB 3%]
```

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

**Sudo apt autoremove**



```
(kali㉿kali)-[~]
$ sudo apt autoremove
REMOVING:
libflac12t64 libgeos3.13.0 libglapi-mesa python3-setproctitle ruby-zeitwerk

Summary:
Upgrading: 0, Installing: 0, Removing: 5, Not Upgrading: 0
Freed space: 5,006 kB

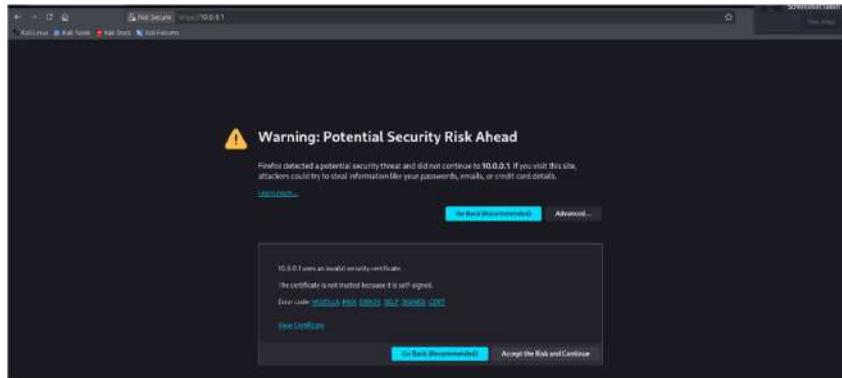
Continue? [Y/n] y
(Reading database ... 411356 files and directories currently installed.)
Removing libflac12t64:amd64 (1.4.3+ds-4) ...
Removing libgeos3.13.0:amd64 (3.13.0-1) ...
Removing libglapi-mesa:amd64 (24.3.4-3) ...
Removing python3-setproctitle:amd64 (1.3.5-1) ...
Removing ruby-zeitwerk (2.6.8-1) ...
Processing triggers for libc-bin (2.40-3) ...
```

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**.

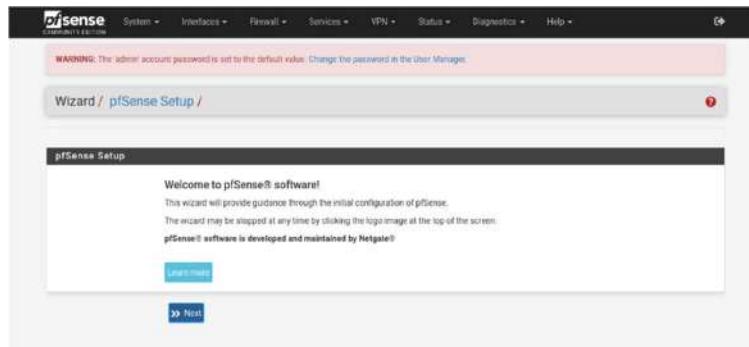


This will open the pfSense Web UI login page. Login using the default credentials.

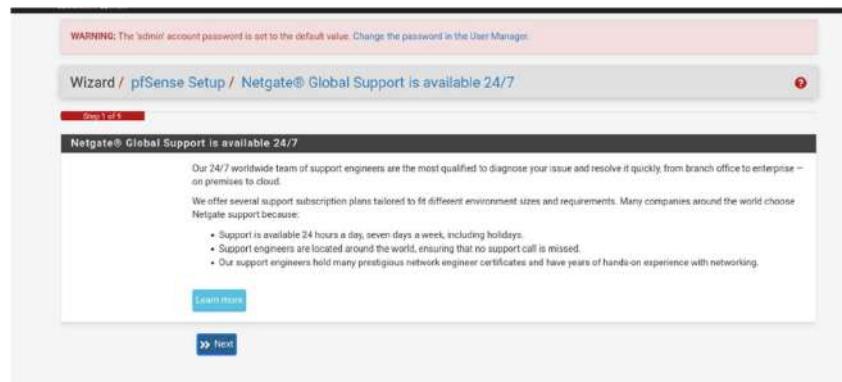
Username: **admin**

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**.

Step 2 of 9

### General Information

On this screen the general pfSense parameters will be set.

**Hostname** pfSense  
Name of the firewall host, without domain part.  
Examples: pfSense, firewall, edgefw

**Domain** security.lab  
Domain name for the firewall.  
Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

**Primary DNS Server**

**Secondary DNS Server**

**Override DNS**  Allow DNS servers to be overridden by DHCP/PPP on WAN

**>> Next**

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

WARNING: The admin account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Time Server Information

Step 3 of 9

### Time Server Information

Please enter the time, date and time zone.

**Time server hostname** 2.pfsense.pool.ntp.org  
Enter the hostname (FQDN) of the time server.

**Timezone** US/Central

**>> Next**

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

Show PPTP password  Reveal password characters

PPTP Local IP Address  apipcalabsoft

PPTP Remote IP Address

PPTP Dial on demand  Enable Dial On-Demand mode  
This option causes the interface to operate in dial-on-demand mode, allowing a virtual full-time connection. The interface is configured, but the actual connection of the line is delayed until qualifying outgoing traffic is detected.

PPTP Idle timeout  If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is brought down. An idle timeout of zero disables this feature.

**RFC1918 Networks**

**Block RFC1918 Private Networks**  Block private networks from entering via WAN  
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10.0/8, 172.16/12, 192.168/16) as well as loopback addresses (127.0.0.1). This option should generally be left turned-on, unless the WAN interface sits in such a private address space, then.

**Block bogon networks**

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

**>> Next**

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

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Configure LAN Interface

Step 5 of 9

Configure LAN Interface

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

LAN IP Address: 10.0.0.1  
Type dhcp if this interface uses DHCP to obtain its IP address.

Subnet Mask: 24

>> Next

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

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Set Admin WebGUI Password

Step 6 of 9

Set Admin WebGUI Password

On this screen the admin password will be set, which is used to access the WebGUI and also SSH services if enabled.

Admin Password: \*\*\*\*\*

Admin Password AGAIN: \*\*\*\*\*

>> Next

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

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Reload configuration

Step 7 of 9

Reload configuration

Click 'Reload' to reload pfSense with new changes.

>> Reload

Click on **Finish**.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Wizard / pfSense Setup / Wizard completed.

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here to learn about Netgate 24/7/365 support services.](#)

User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous).

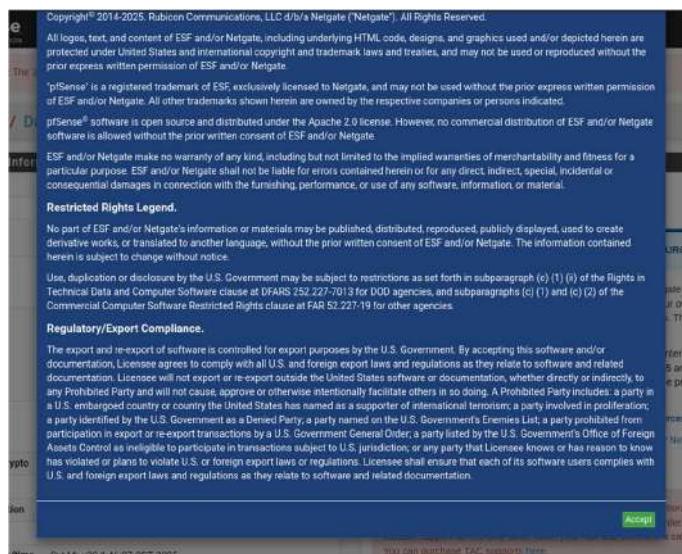
[Anonymous User Survey](#)

Useful resources.

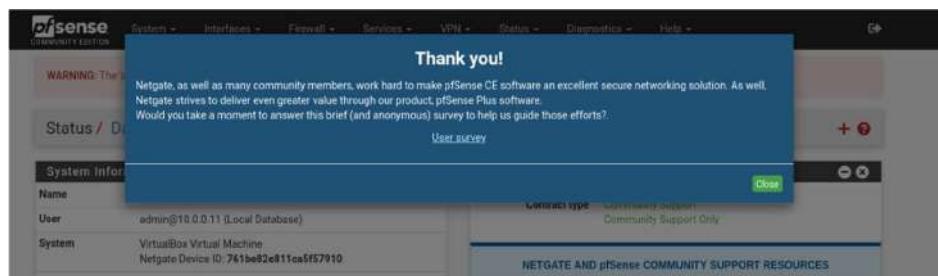
- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, visit our [store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.

>> Finish

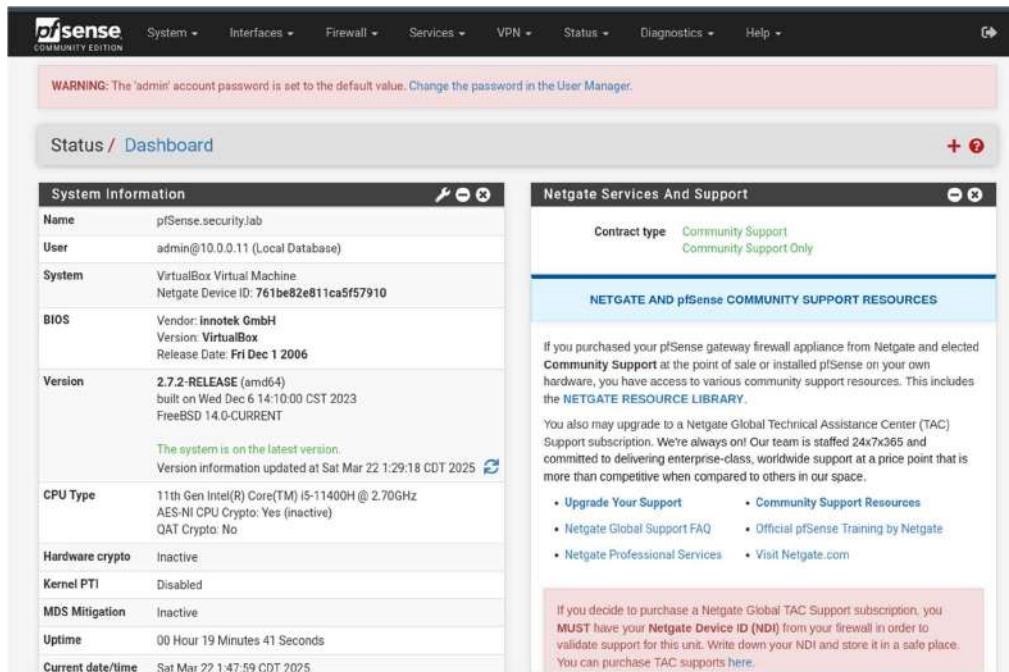
Click accept



Then click close

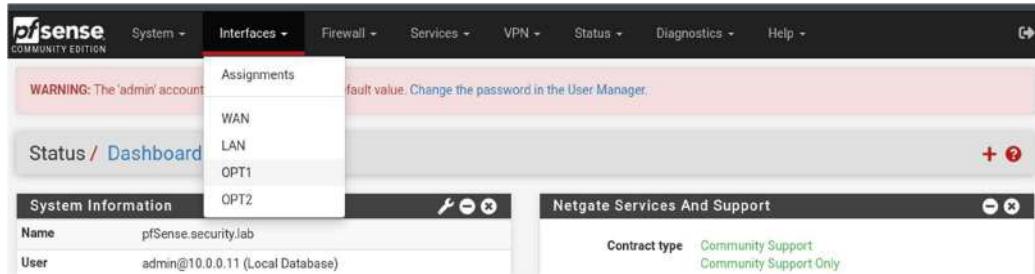


After interface looks like this



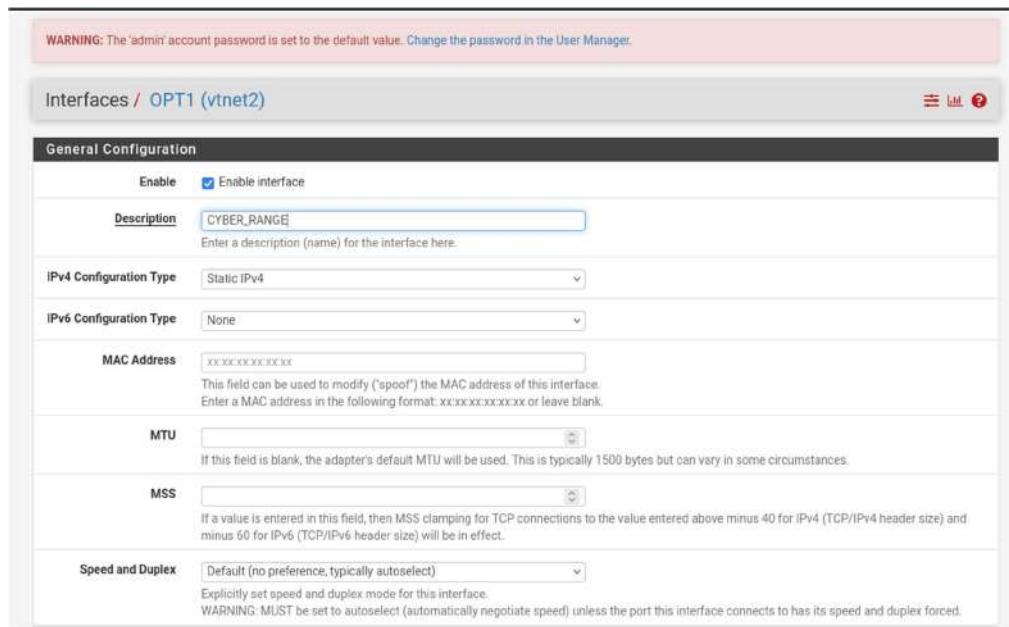
## Interface Renaming

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



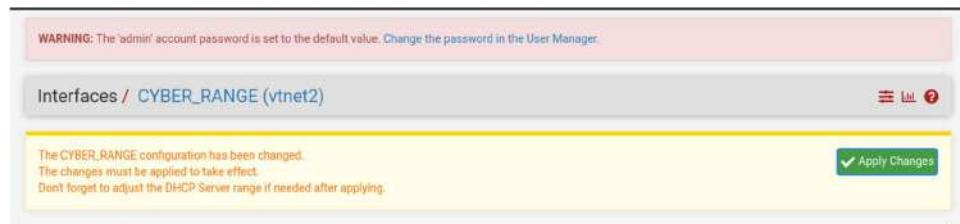
The screenshot shows the pfSense interface with the 'Interfaces' menu open. The 'OPT1' interface is selected. A warning message at the top left says: 'WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.' The 'System Information' section shows the name as 'pfSense.security.lab' and the user as 'admin@10.0.0.11 (Local Database)'. A 'Netgate Services And Support' box indicates 'Community Support' and 'Community Support Only'.

In the Description field enter **CYBER\_RANGE**. Scroll to the bottom and click on **Save**.



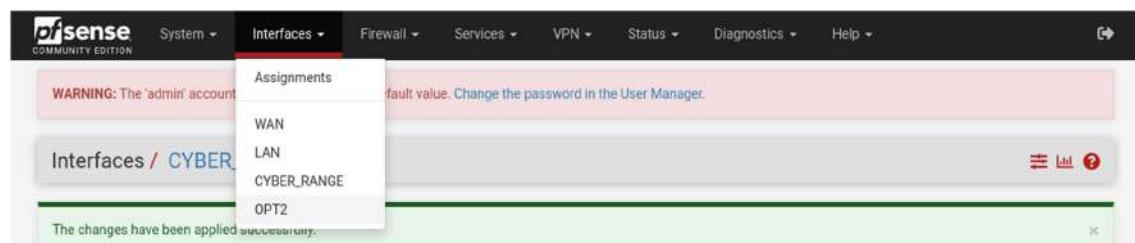
The screenshot shows the 'General Configuration' page for the 'OPT1 (vtnet2)' interface. The 'Description' field is set to 'CYBER\_RANGE'. Other settings include 'Enable' checked, 'IPv4 Configuration Type' as 'Static IPv4', and 'MAC Address' as '00:0C:00:00:00:00'. The 'Speed and Duplex' dropdown is set to 'Default (no preference, typically autoselect)'. A note at the bottom says: 'Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.'

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



The screenshot shows a confirmation dialog box with the message: 'The CYBER\_RANGE configuration has been changed. The changes must be applied to take effect. Don't forget to adjust the DHCP Server range if needed after applying.' A green 'Apply Changes' button with a checkmark is visible.

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



The screenshot shows the pfSense interface with the 'Interfaces' menu open. The 'OPT2' interface is selected. A message at the bottom left says: 'The changes have been applied successfully.' The 'System Information' section shows the name as 'pfSense.security.lab' and the user as 'admin@10.0.0.11 (Local Database)'. A 'Netgate Services And Support' box indicates 'Community Support' and 'Community Support Only'.

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

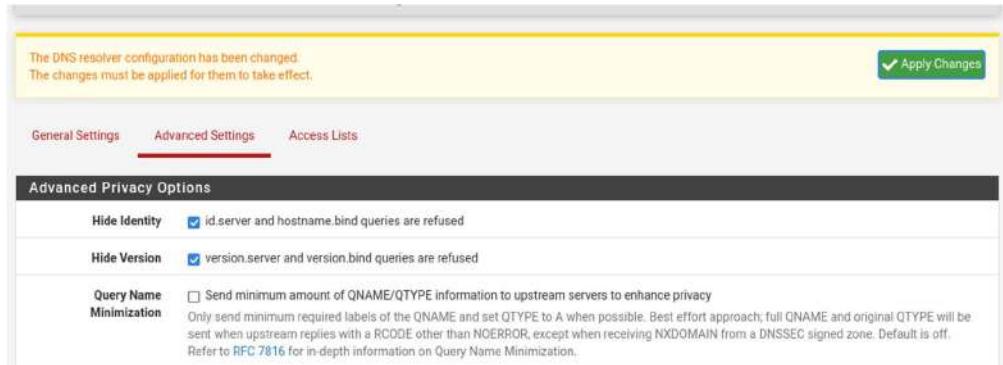
A popup will appear at the top of the page click on **Apply Changes**.

## DNS Resolver Configuration

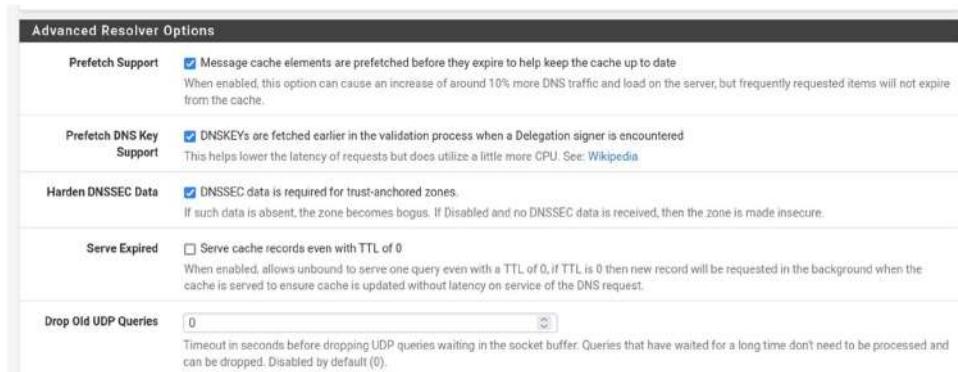
From the navigation bar select **Services -> DNS Resolver**.

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.

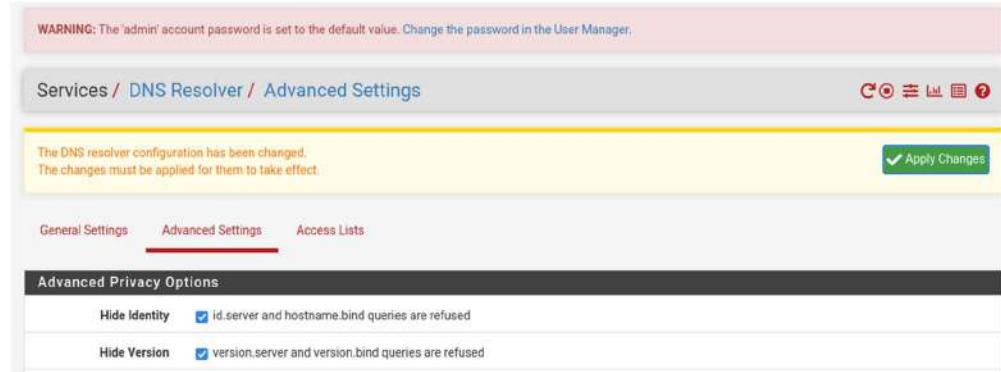
Click on **Advanced Settings**.



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



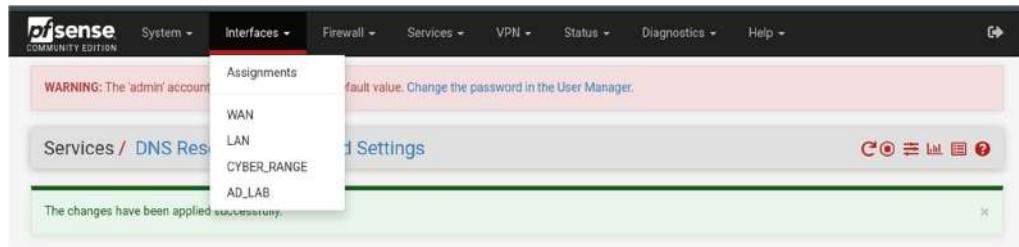
A popup will appear at the top of the page. Click on **Apply Changes**.



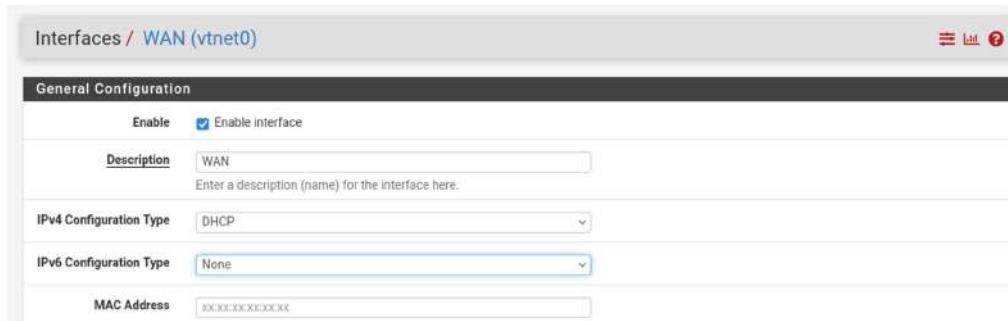
## Disabling DHCPv6

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.

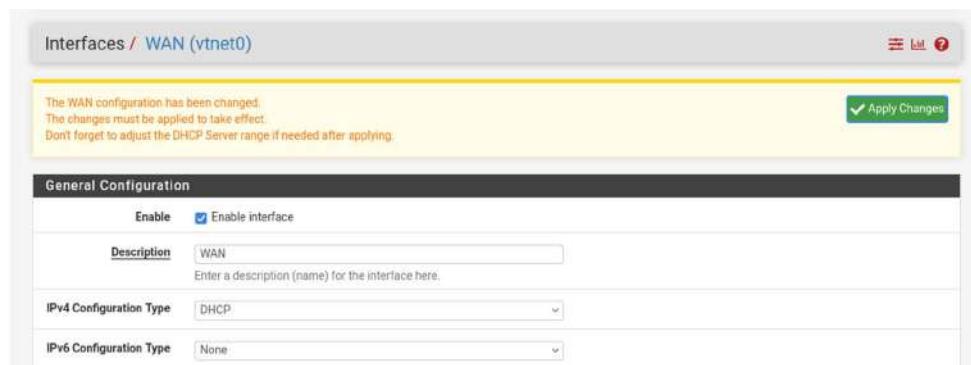
From the navigation bar select **Interfaces -> WAN**.



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



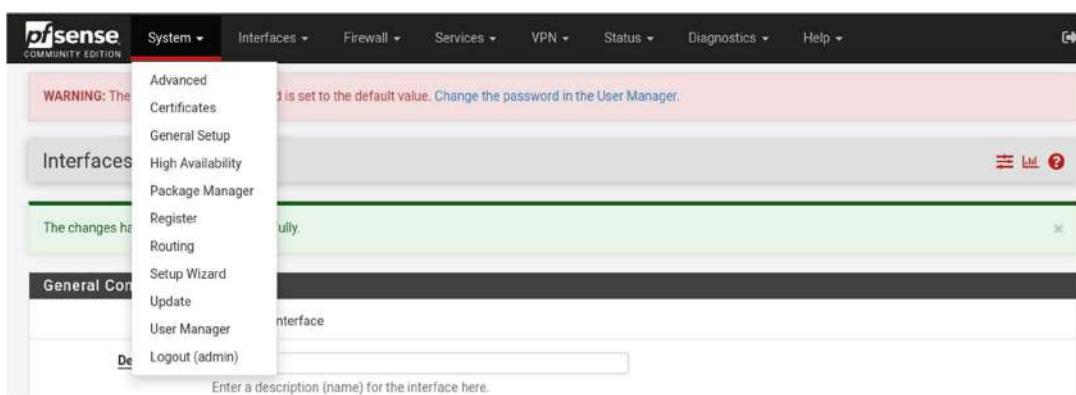
At the top of the page, a new popup will appear. Click on **Apply Changes**.



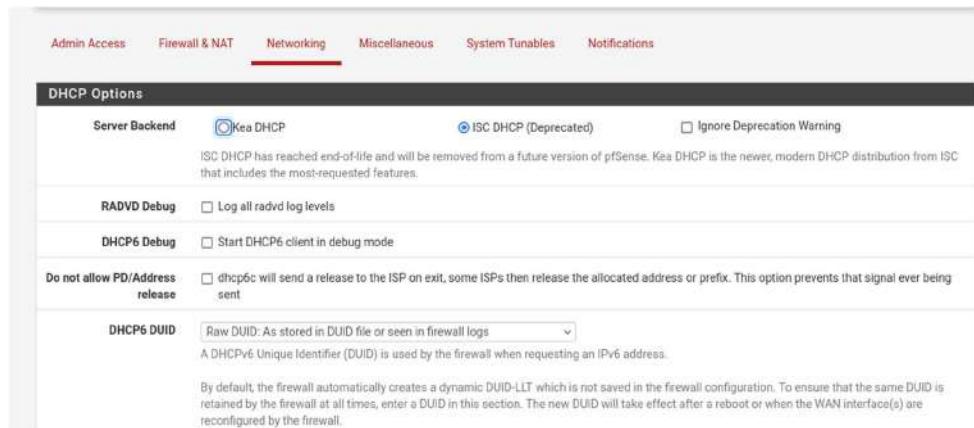
Restart the pfSense VM. Now, the WAN interface should have an IPv4 address.

## Advanced Configuration

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

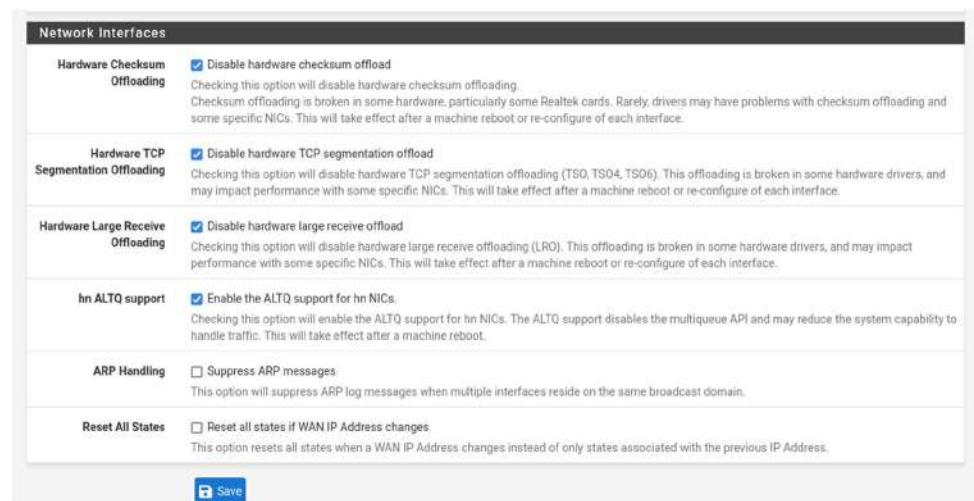


Go to the **Networking** tab



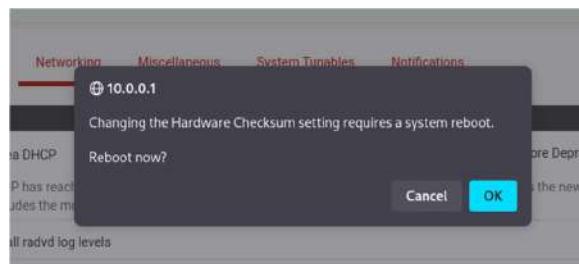
The screenshot shows the Networking tab selected in the top navigation bar. The sub-section shown is 'DHCP Options'. It includes settings for the 'Server Backend' (Kea DHCP selected, ISC DHCP (Deprecated) is deprecated), RADVD and DHCP6 Debug checkboxes, and a 'Do not allow PD/Address release' checkbox. There is also a 'DHCP6 DUID' section with a dropdown and a note about retaining the DUID across reboots.

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**.



The screenshot shows the 'Network Interfaces' section. Under 'Hardware Checksum Offloading', the 'Disable hardware checksum offload' checkbox is checked. Other sections like 'Hardware TCP Segmentation Offloading', 'Hardware Large Receive Offloading', and 'hn ALTQ support' also have their respective checkboxes checked. A 'Save' button is at the bottom.

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



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



The screenshot shows the 'Diagnostics / Reboot' page. It displays the message 'Rebooting' and 'Page will automatically reload in 86 seconds'.

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**.

pfSense  
COMMUNITY EDITION

System / Dashboard

**System Information**

Name	pfSense.security.lab
User	admin@10.0.0.11 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: 761be82e811ca5f57910
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 14:10:00 CST 2023 FreeBSD 14.0-CURRENT
CPU Type	11th Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz AES-NI CPU Crypto: Yes (inactive) CPU Counter: No

**Status**

- Captive Portal
- CARP (failover)
- Dashboard
- DHCP Leases**
- DHCPv6 Leases
- DNS Resolver
- Filter Reload
- Gateways
- Interfaces
- IPsec
- Monitoring
- NTP
- OpenVPN
- Queues
- Services
- System Logs
- Traffic Graph

**Support**

- Community Support
- Community Support Only

**pfSense COMMUNITY SUPPORT RESOURCES**

- Get support from the pfSense community and the Netgate firewall appliance from Netgate and elected point of sale or installed pfSense on your own
- Netgate Global Technical Assistance Center (TAC)
- Netgate Global Support Team
- Netgate Global Support FAQ
- Community Support Resources
- Official pfSense Training by Netgate

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.

Search

Search Term:  All

Enter a search string or \*nix regular expression to filter entries.

**Leases**

IP Address	MAC Address	Hostname	Description	Start	End	Actions
10.0.0.11	08:00:27:04:42:0f	kali		2025/03/22 06:29:02	2025/03/22 08:29:02	<input type="button" value="+"/>

**Lease Utilization**

Interface	Pool Start	Pool End	Used	Capacity	Utilization
LAN	10.0.0.10	10.0.0.245	1	236	0% of 236

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

Static DHCP Mapping on LAN

DHCP Backend: ISC DHCP

MAC Address: 08:00:27:04:42:0f

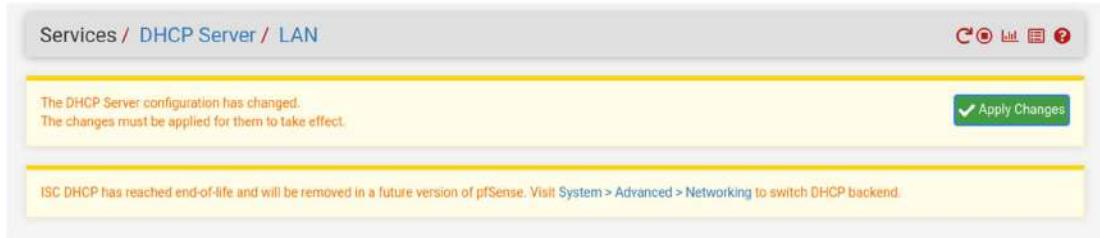
Client Identifier: An optional identifier to match based on the value sent by the client (RFC 2132).

IP Address: 10.0.0.2

IPv4 address to assign this client.

Address must be outside of any defined pools. If no IPv4 address is given, one will be dynamically allocated from a pool. The same IP address may be assigned to multiple mappings.

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



The screenshot shows the pfSense LAN configuration page. At the top, there is a message: "The DHCP Server configuration has changed. The changes must be applied for them to take effect." Below this, there is a note: "ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend." On the right side of the message box is a green "Apply Changes" button with a checkmark icon.

## Refresh Kali Linux IP Address

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

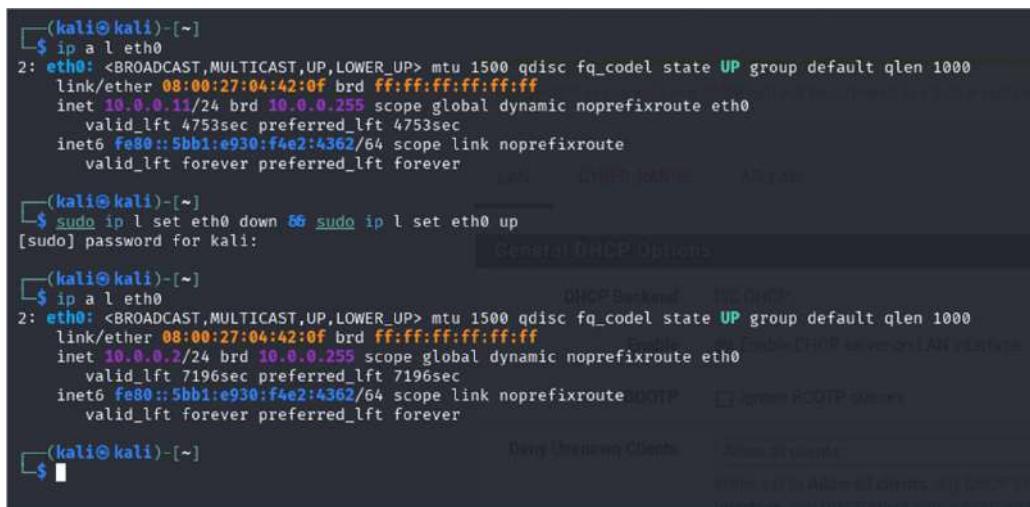
```
ip a l eth0
```

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
```



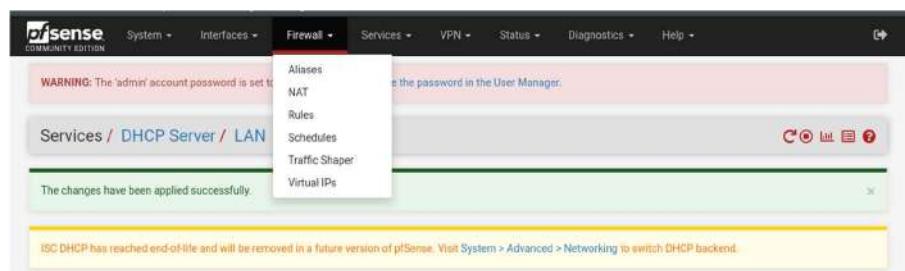
The terminal window shows the following sequence of commands and output:

```
(kali㉿kali)-[~]
$ ip a l eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.11/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
      valid_lft 4753sec preferred_lft 4753sec
    inet6 fe80::5bb1:e930:f4e2:4362/64 scope link noprefixroute
      valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ sudo ip l set eth0 down && sudo ip l set eth0 up
[sudo] password for kali:
(kali㉿kali)-[~]
$ ip a l eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.2/24 brd 10.0.0.255 scope global dynamic noprefixroute eth0
      valid_lft 7196sec preferred_lft 7196sec
    inet6 fe80::5bb1:e930:f4e2:4362/64 scope link noprefixroute
      valid_lft forever preferred_lft forever
```

## pfSense Firewall Configuration

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

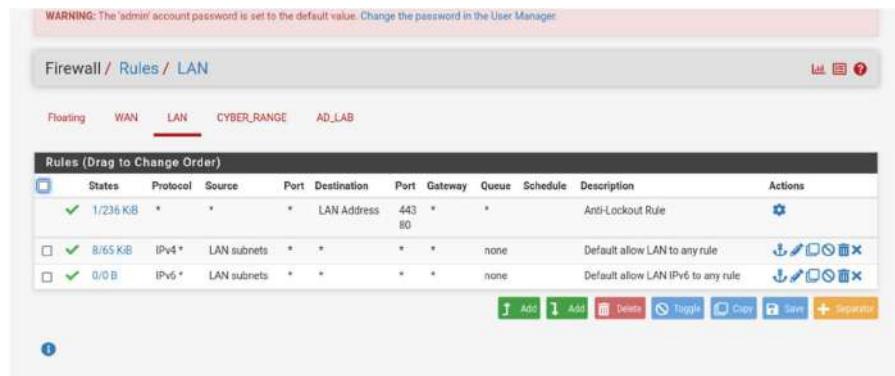


The screenshot shows the pfSense Firewall Rules configuration page. At the top, there is a message: "WARNING: The 'admin' account password is set to 'admin'. Please change the password in the User Manager." Below this, there is a green message box: "The changes have been applied successfully." On the right side of the message box is a note: "ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit System > Advanced > Networking to switch DHCP backend." The navigation bar shows the user is in the Firewall section, with sub-options for Aliases, NAT, Rules, Schedules, Traffic Shaper, and Virtual IP's.

## 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.



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / LAN

Floating WAN LAN CYBER\_RANGE AD\_LAB

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/236 KB	*	*	*	LAN Address	443	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 8/65 KB	IPv4	*	*	LAN subnets	*	*	*	*	Default allow LAN to any rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv6	*	*	LAN subnets	*	*	*	*	Default allow LAN IPv6 to any rule	

Add rule to top Add Delete Toggle Copy Save Separate

Change the following options:

Action: **Block**

Address Family: **Ipv4+Ipv6**

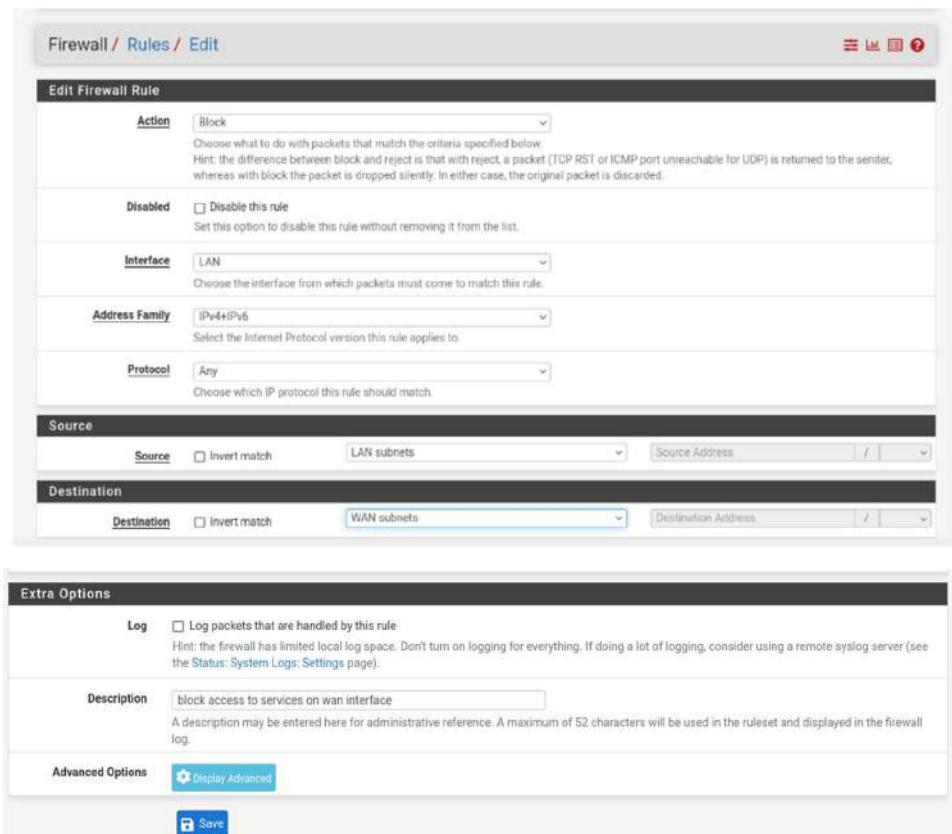
Protocol: **Any**

Source: **LAN subnets**

Destination: **WAN subnets**

Description: **Block access to services on WAN interface**

click on Save.



Firewall / Rules / Edit

Edit Firewall Rule

Action: **Block**

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled:  Disable this rule  
Set this option to disable this rule without removing it from the list.

Interface: **LAN**  
Choose the interface from which packets must come to match this rule.

Address Family: **IPv4+IPv6**  
Select the Internet Protocol version this rule applies to.

Protocol: **Any**  
Choose which IP protocol this rule should match.

Source

Source:  Invert match **LAN subnets**  Source Address /

Destination

Destination:  Invert match **WAN subnets**  Destination Address /

Extra Options

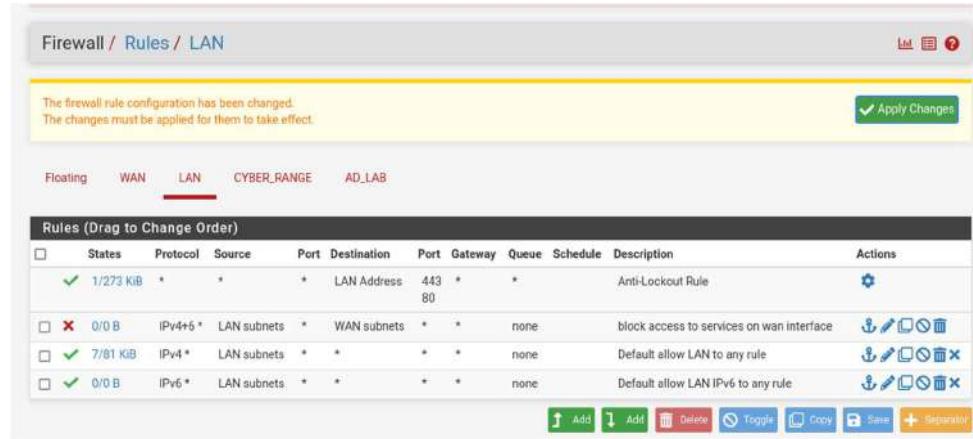
Log:  Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: **block access to services on wan interface**  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options 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 screenshot shows the pfSense Firewall / Rules / LAN interface. At the top, a yellow banner displays the message: "The firewall rule configuration has been changed. The changes must be applied for them to take effect." To the right of the banner is a green "Apply Changes" button with a checkmark. Below the banner, the navigation bar includes tabs for Floating, WAN, LAN (which is selected and highlighted in red), CYBER\_RANGE, and AD\_LAB. The main content area is titled "Rules (Drag to Change Order)" and contains a table of rules. The table has columns for: States, Protocol, Source, Port, Destination, Port, Gateway, Queue, Schedule, Description, and Actions. There are four rules listed:

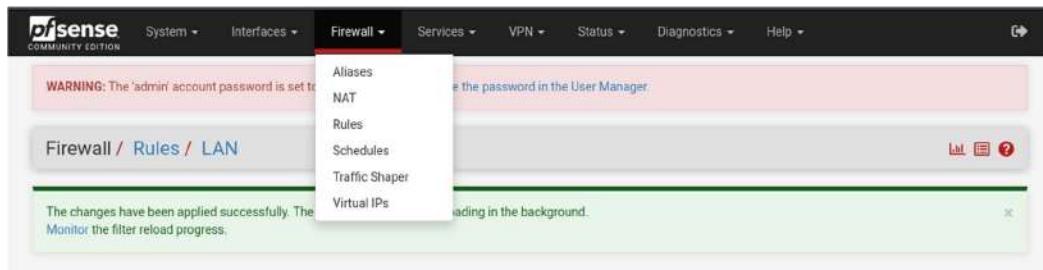
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/273 KIB	*	*	*	LAN Address 80	443	*	*		Anti-Lockout Rule	
✗ 0/0 B	IPv4+5	LAN subnets	*	WAN subnets	*	*	none		block access to services on wan interface	
✓ 7/81 KIB	IPv4	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

At the bottom of the interface are several action buttons: Add, Add, Delete, Toggle, Copy, Save, and Import.

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**.



The screenshot shows the pfSense Firewall / Rules / LAN interface. The navigation bar is visible with the "Firewall" tab selected. A dropdown menu for "Firewall" is open, showing the following options: Aliases, NAT, Rules, Schedules, Traffic Shaper, and Virtual IPs. The "Aliases" option is highlighted. A yellow banner at the top of the main content area says: "WARNING: The 'admin' account password is set to 'admin'. Please change the password in the User Manager." Below the banner, the title "Firewall / Rules / LAN" is displayed. A message in the center of the screen says: "The changes have been applied successfully. The filter reload is in progress. Monitor the filter reload progress." At the bottom of the interface are several action buttons: Add, Add, Delete, Toggle, Copy, Save, and Import.

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



The screenshot shows the pfSense Firewall / Aliases / IP interface. The navigation bar is visible with the "IP" tab selected. A dropdown menu for "IP" is open, showing the following options: IP, Ports, URLs, and All. The "IP" option is highlighted. The main content area is titled "Firewall Aliases IP" and contains a table of aliases. The table has columns for: Name, Type, Values, Description, and Actions. There is one row in the table:

Name	Type	Values	Description	Actions
RFC1918	Network(s)	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 169.254.0.0/16, 127.0.0.0/8		

At the bottom of the interface are several action buttons: Add, Import.

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.

Firewall / Aliases / Edit

**Properties**

Name	RFC1918	The name of the alias may only consist of the characters 'a-z, A-Z, 0-9 and _*.'
Description	Private ipv4 address space	A description may be entered here for administrative reference (not parsed).
Type	Network(s)	

**Network(s)**

Hint: Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. An IP range such as 192.168.1.1-192.168.1.254 may also be entered and a list of CIDR networks will be derived to fill the range.

Network or FQDN	10.0.0.0	/ 8	Description	
	172.16.0.0	/ 12	Description	
	192.168.0.0	/ 16	Description	
	169.254.0.0	/ 16	Description	
	127.0.0.0	/ 8	Description	

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

The final result should be as follows:

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Aliases / IP

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

**Firewall Aliases IP**

Name	Type	Values	Description	Actions
RFC1918	Network(s)	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 169.254.0.0/16, 127.0.0.0/8	Private ipv4 address space	

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

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Aliases / IP

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

**Aliases**

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

Select the **CYBER\_RANGE** tab.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / CYBER\_RANGE

Floating WAN LAN CYBER\_RANGE AD\_LAB

**Rules (Drag to Change Order)**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.										

Use the “Add rule to end” button for all the rules.

Configure the rule as follows: Address Family: **IPv4+IPv6**

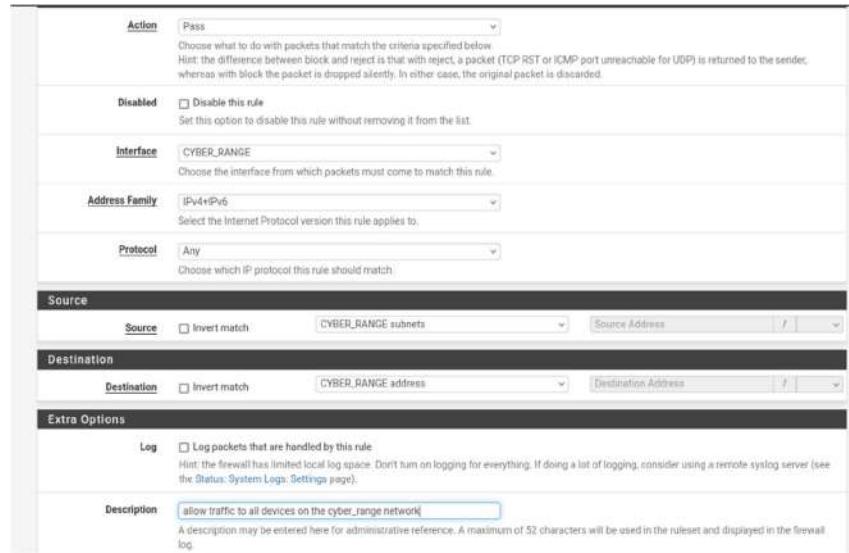
Protocol: **Any**

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**.



The screenshot shows the configuration for the first rule. The 'Action' dropdown is set to 'Pass'. Under 'Source', the 'Address Family' is 'IPv4+IPv6', 'Protocol' is 'Any', and 'Source' is 'CYBER\_RANGE subnets'. Under 'Destination', 'Destination' is 'CYBER\_RANGE address'. In the 'Extra Options' section, the 'Description' is 'allow traffic to all devices on the cyber\_range network'.

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:

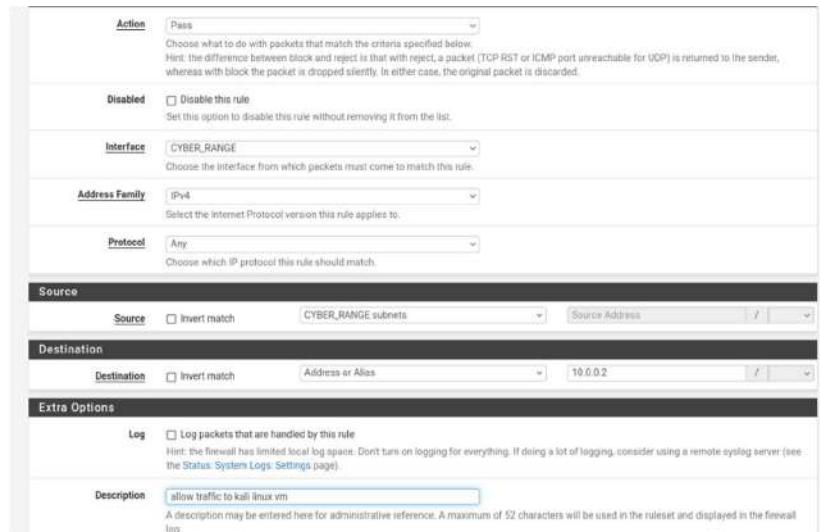
Protocol: **Any**

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**.



The screenshot shows the configuration for the second rule. The 'Action' dropdown is set to 'Pass'. Under 'Source', the 'Address Family' is 'IPv4', 'Protocol' is 'Any', and 'Source' is 'CYBER\_RANGE subnets'. Under 'Destination', 'Destination' is 'Address or Alias' with value '10.0.0.2'. In the 'Extra Options' section, the 'Description' is 'allow traffic to kali linux vm'.

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**.

Action: Pass  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled:  Disable this rule  
Set this option to disable this rule without removing it from the list.

Interface: CYBER\_RANGE  
Choose the interface from which packets must come to match this rule.

Address Family: IPv4  
Select the Internet Protocol version this rule applies to.

Protocol: Any  
Choose which IP protocol this rule should match.

**Source**

Source:  Invert match CYBER\_RANGE subnets / Source Address

**Destination**

Destination:  Invert match Address or Alias RFC1918 /

**Extra Options**

Log:  Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: allow to any non-private ipv4 address  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

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**.

**Edit Firewall Rule**

<b>Action</b>	Block	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.			
<b>Disabled</b>	<input type="checkbox"/> Disable this rule	Set this option to disable this rule without removing it from the list.			
<b>Interface</b>	CYBER_RANGE	Choose the interface from which packets must come to match this rule.			
<b>Address Family</b>	IPv4+IPv6	Select the Internet Protocol version this rule applies to.			
<b>Protocol</b>	Any	Choose which IP protocol this rule should match.			
<b>Source</b>					
Source	<input type="checkbox"/> Invert match	CYBER_RANGE subnets	Source Address	<input type="text"/>	
<b>Destination</b>					
Destination	<input type="checkbox"/> Invert match	Any	Destination Address	<input type="text"/>	
<b>Extra Options</b>					
<b>Log</b>	<input type="checkbox"/> Log packets that are handled by this rule	Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).			
<b>Description</b>					
block access to everything					

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

The final rules should look as follows:

**Firewall / Rules / CYBER\_RANGE**

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

**Apply Changes**

Floating	WAN	LAN	CYBER_RANGE	AD_LAB						
<b>Rules (Drag to Change Order)</b>										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4+6 *	CYBER_RANGE subnets	*	CYBER_RANGE address	*	*	none	allow traffic to all devices on the cyber_range network	
<input type="checkbox"/>	0/0 B	IPv4 *	CYBER_RANGE subnets	*	10.0.0.2	*	*	none	allow traffic to kali linux vm	
<input type="checkbox"/>	0/0 B	IPv4 *	CYBER_RANGE subnets	*	!RFC1918	*	*	none	allow to any non-private ipv4 address	
<input type="checkbox"/>	0/0 B	IPv4+6 *	CYBER_RANGE subnets	*	*	*	*	none	block access to everything	

**Add** **Up** **Down** **Delete** **Toggle** **Copy** **Save** **Separator**

## AD\_LAB Rules

Click on the **AD\_LAB** tab. Use the “Add rule to end” button to create new rules.

**WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.**

**Firewall / Rules / AD\_LAB**

Floating	WAN	LAN	CYBER_RANGE	AD_LAB						
<b>Rules (Drag to Change Order)</b>										
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rules are currently defined for this interface. All incoming connections on this interface will be blocked until new rules are added. Click the button to add a new rule.										
<b>Add</b> <b>Up</b> <b>Down</b> <b>Delete</b> <b>Toggle</b> <b>Copy</b> <b>Save</b> <b>Separator</b>										

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**.



Action: Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled:  Disable this rule  
Set this option to disable this rule without removing it from the list.

Interface: AD\_LAB

Address Family: IPv4+IPv6

Protocol: Any

Source: Source:  Invert match AD\_LAB subnets

Destination: Destination:  Invert match WAN subnets

Extra Options: Log:  Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).  
Description: Block access to services on wan interface  
A description may be entered here for administrative reference. A maximum of 512 characters will be used in the rule and displayed in the firewall log.

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**

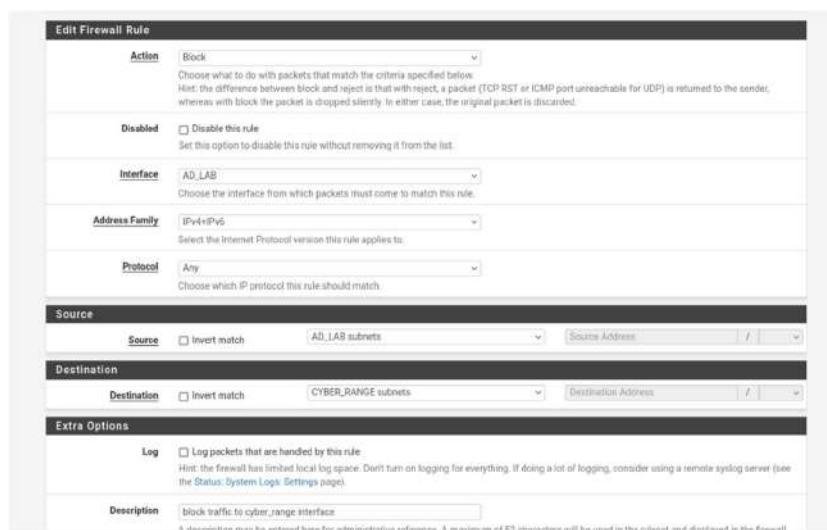
Protocol: **Any**

Source: **AD\_LAB subnets**

Destination: **CYBER\_RANGE subnets**

Description: **Block traffic to CYBER\_RANGE interface**

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



Action: Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled:  Disable this rule  
Set this option to disable this rule without removing it from the list.

Interface: AD\_LAB

Address Family: IPv4+IPv6

Protocol: Any

Source: Source:  Invert match AD\_LAB subnets

Destination: Destination:  Invert match CYBER\_RANGE subnets

Extra Options: Log:  Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).  
Description: block traffic to cyber\_range interface  
A descriptive text has been added here for administrative reference. A maximum of 512 characters will be used in the rule and displayed in the firewall log.

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

The rule has the following details:

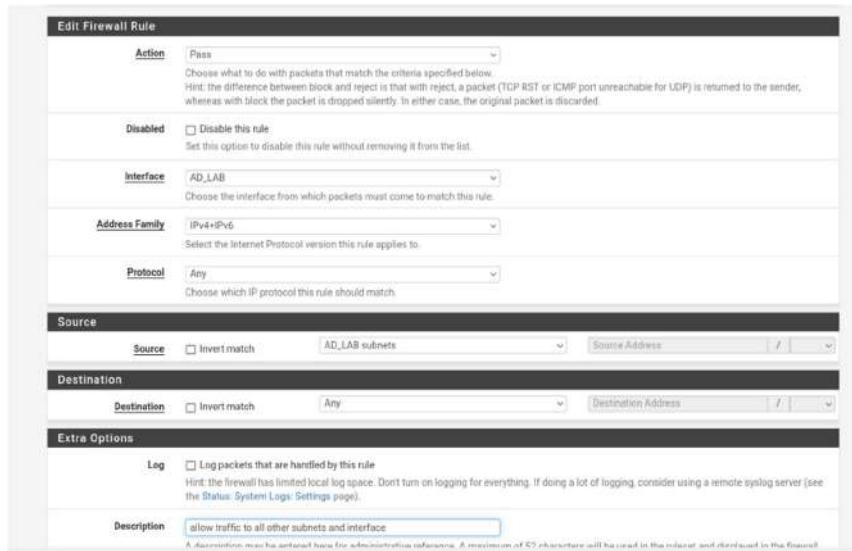
Address Family: **IPv4+IPv6**

Protocol: **Any**

Source: **AD\_LAB subnets**

Description: **Allow traffic to all other subnets and Internet**

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



Action: Pass

Disabled:  Disable this rule

Interface: AD\_LAB

Address Family: IPv4+IPv6

Protocol: Any

Source: Source  Invert match AD\_LAB subnets

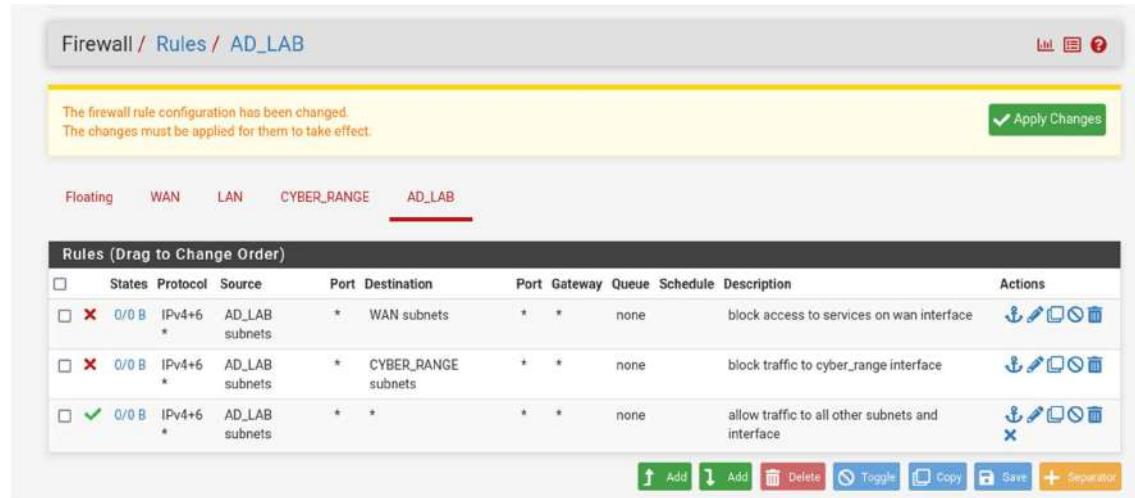
Destination: Destination  Invert match Any

Extra Options: Log  Log packets that are handled by this rule

Description: allow traffic to all other subnets and interface

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

The final rules should look as follows:



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

Apply Changes

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0/0 B	IPv4+6	AD_LAB subnets	*	WAN subnets	*	*	none		block access to services on wan interface	
<input type="checkbox"/>	0/0 B	IPv4+6	AD_LAB subnets	*	CYBER_RANGE subnets	*	*	none		block traffic to cyber_range interface	
<input checked="" type="checkbox"/>	0/0 B	IPv4+6	AD_LAB subnets	*	*	*	*	none		allow traffic to all other subnets and interface	

Add Add Delete Toggle Copy Save Separate

pfSense Reboot

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

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / AD\_LAB

The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.

Floating WAN LAN CYBER\_RANGE AD\_LAB

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule
<input type="checkbox"/>	0/0 B	IPv4+6	*	*	AD_LAB subnets	*	*	none	
<input type="checkbox"/>	0/0 B	IPv4+6	*	*	AD_LAB subnets	*	*	none	
<input type="checkbox"/>	0/0 B	IPv4+6	*	*	CYBER_RANGE subnets	*	*	none	
<input checked="" type="checkbox"/>	0/0 B	IPv4+6	*	*	AD_LAB subnets	*	*	none	

Add Toggle Copy Save Delete

ARP Table Authentication Backup & Restore Command Prompt DNS Lookup Edit File Factory Defaults Halt System Limiter Info NDP Table Packet Capture

Click on Submit.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Diagnostics / Reboot

Select reboot method

Reboot method: Normal reboot

Select "Normal reboot" to reboot the system immediately, or "Reroot" to stop processes, remount disks and re-run startup sequence.

Submit

## CYBER RANGE-Metasploit installation

Download Metasploitable 2

Go to the following URL: [Metasploitable: 2 ~ VulnHub](https://www.vulnhub.com/entry/metasploitable-2-11/) 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**.

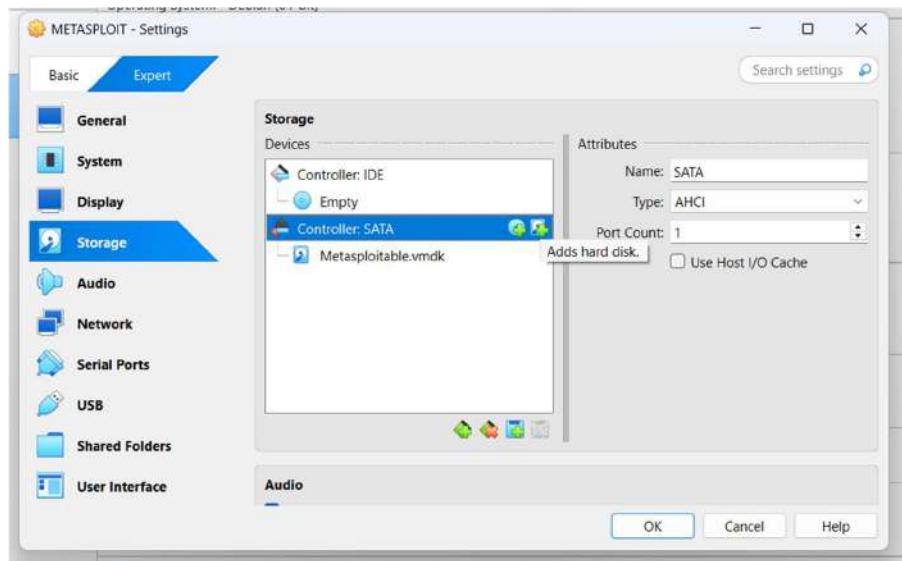
All my VMs for the Home Lab project are located in **D:\Virtual Machines**. Whenever we create a new group in VirtualBox a corresponding folder is created on the filesystem to store the VM.

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**.

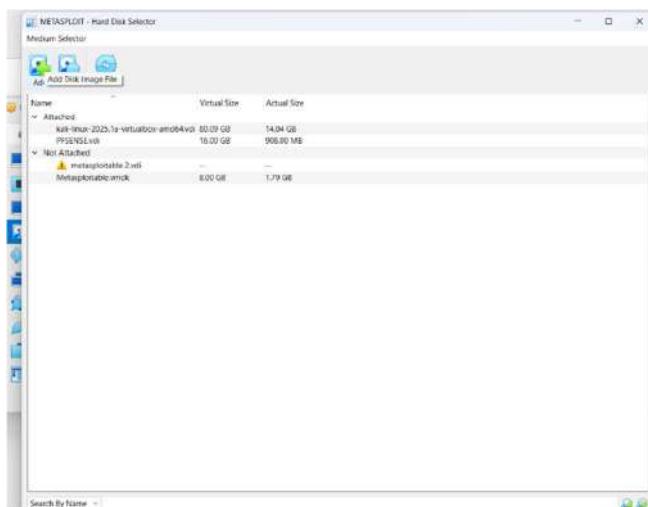
Find the Metasploitable VM folder location in your case and move the downloaded **.vmdk** into it.

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

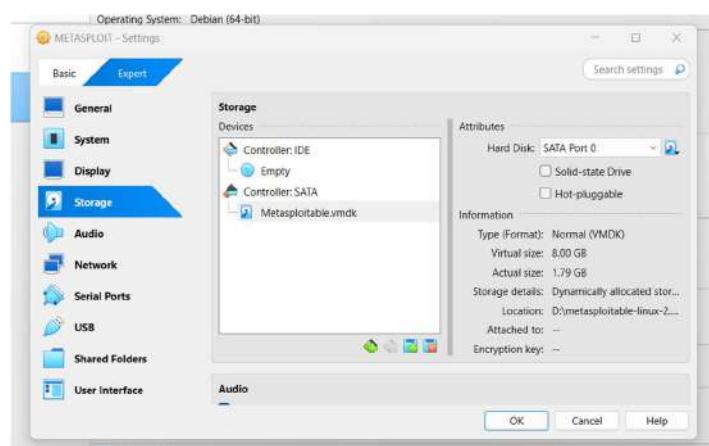
Go to **Storage** and select **Controller: SATA** then click on the small “Add Hard Disk” icon on the right.



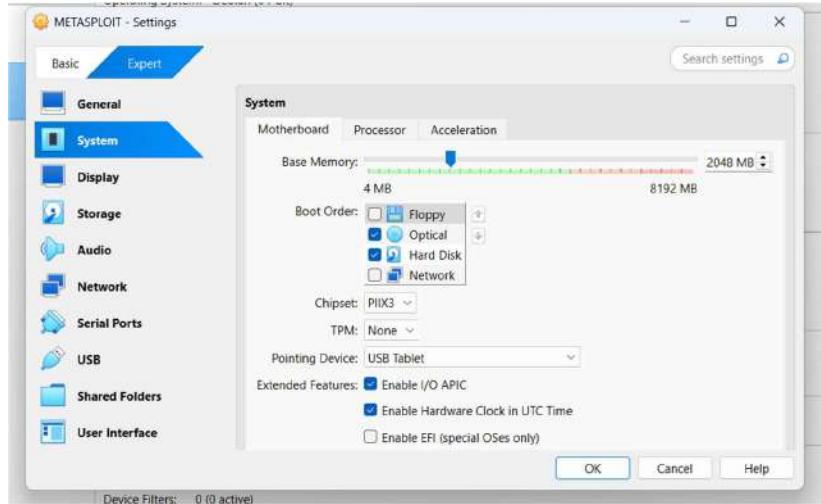
This will open the Hard Disk Selector menu. Click on Add and then select the **.vmdk** file. Then click on the Choose button to use the Hard Drive.



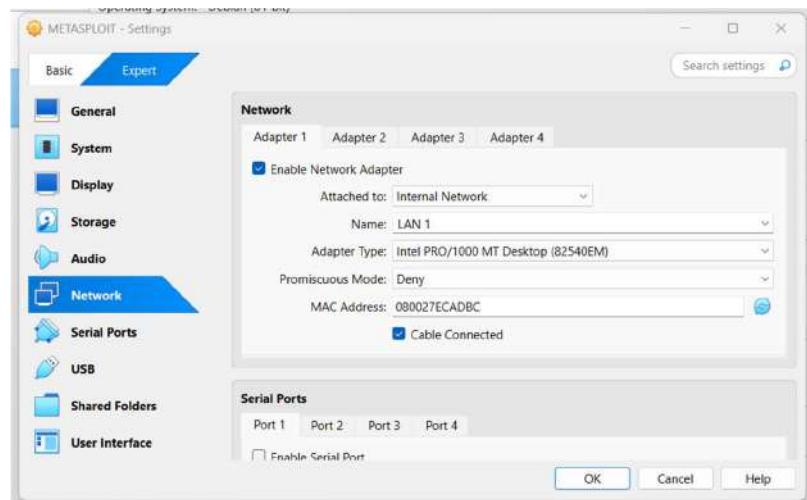
If done correctly under **Controller: SATA** the Hard Disk will be visible.



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 Attached 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](https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019)

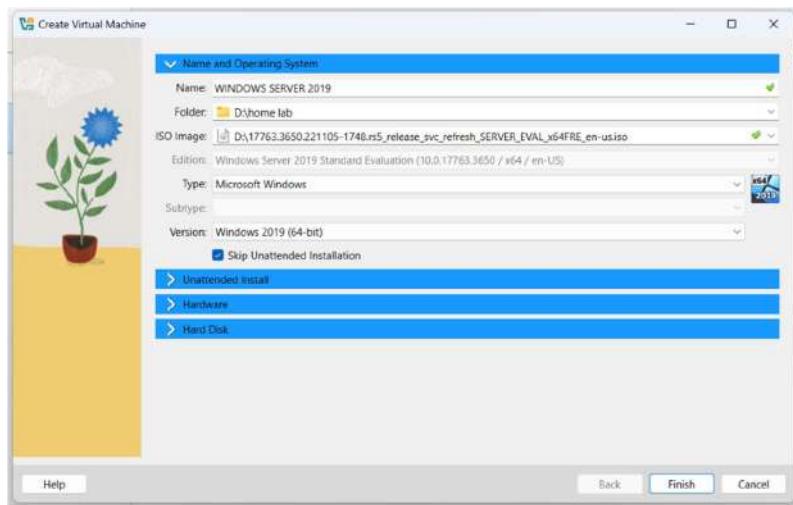
Click on the **64-bit edition** download. The ISO file is ~5GB.

### Creating the VM

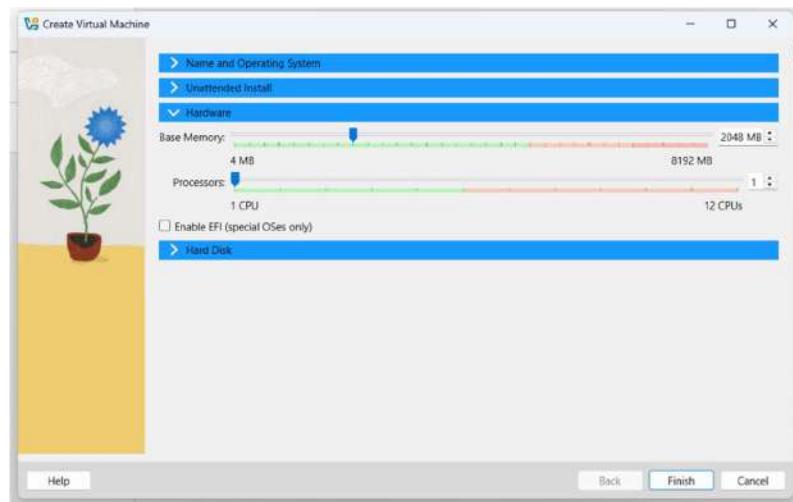
Windows Server 2019

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

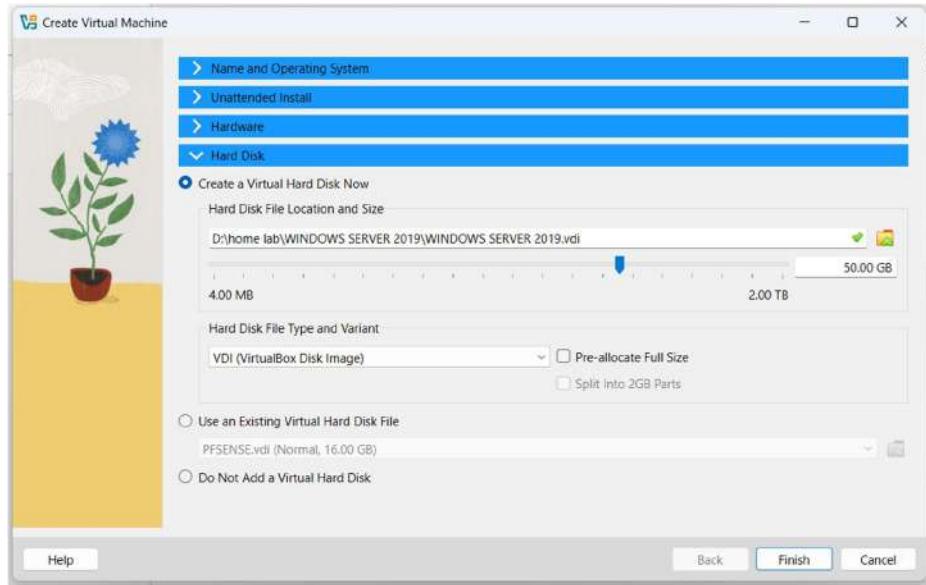
Gave the VM a name. Ensure that the Folder option points to the location where all the Home Lab-related VMs are saved. For the ISO Image select the downloaded Windows Server 2019 image. Select the **Skip Unattended Installation** option and then click on **Next**.



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



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

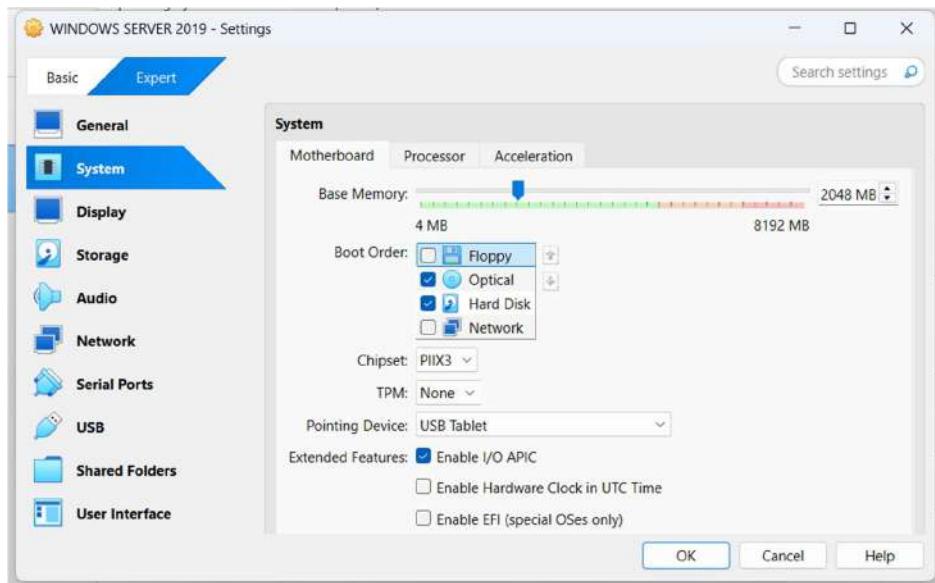


## Configuring the VM

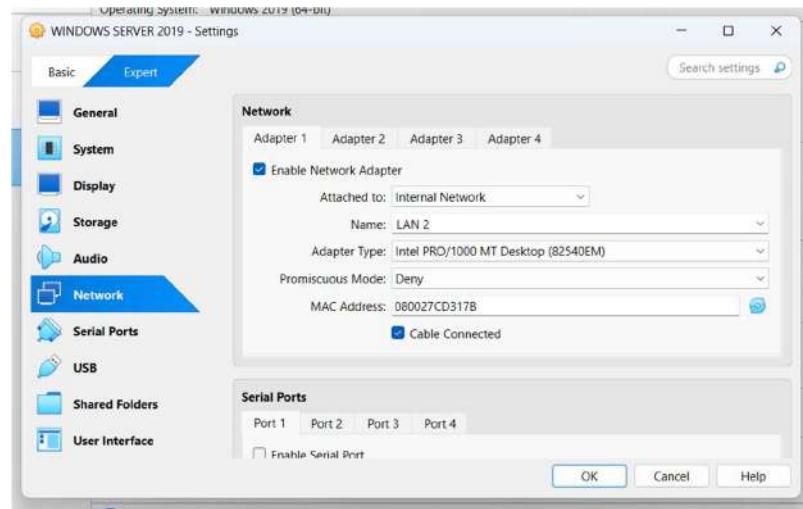
### Windows Server 2019

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 Attached to field select **Internal Network**. For name select **LAN 2**. Click on **OK** to save the settings.

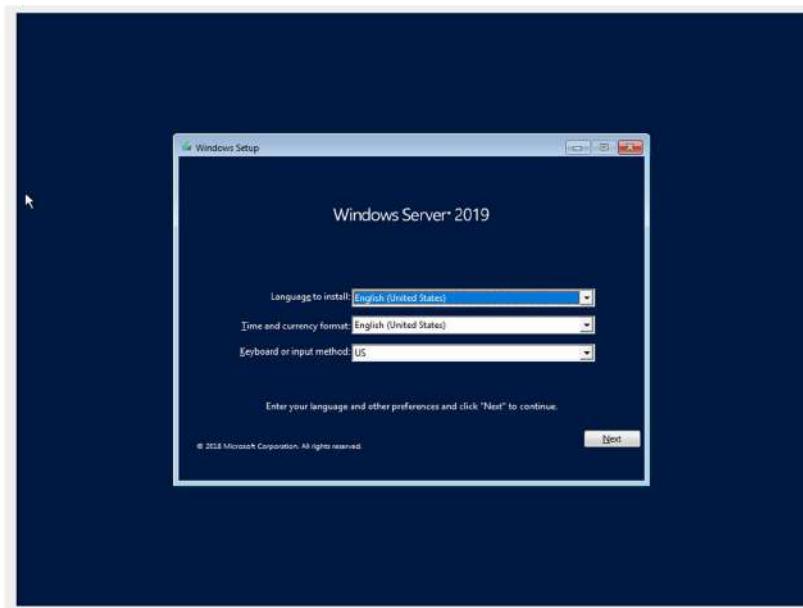


## Windows Server 2019 Setup

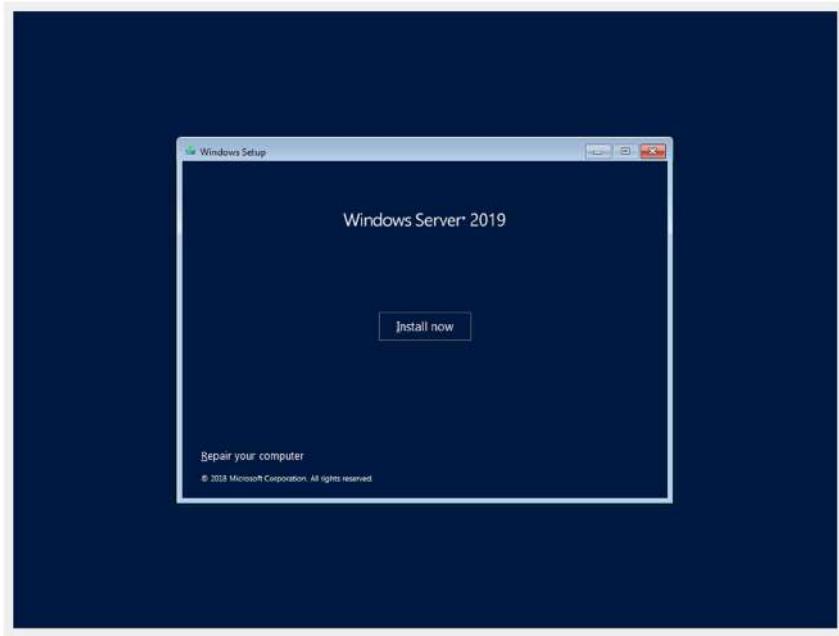
### OS Installation

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

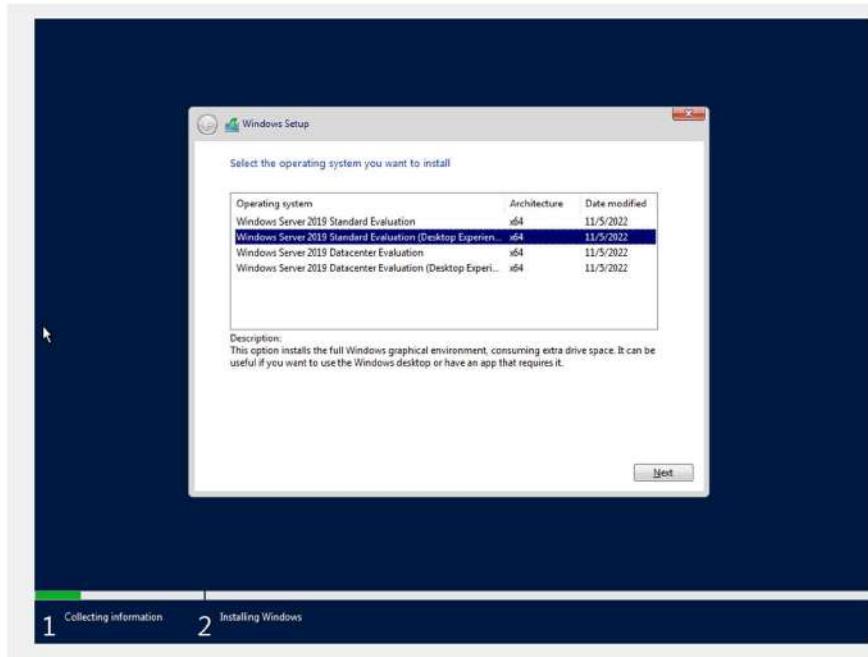
Click on **Next**.



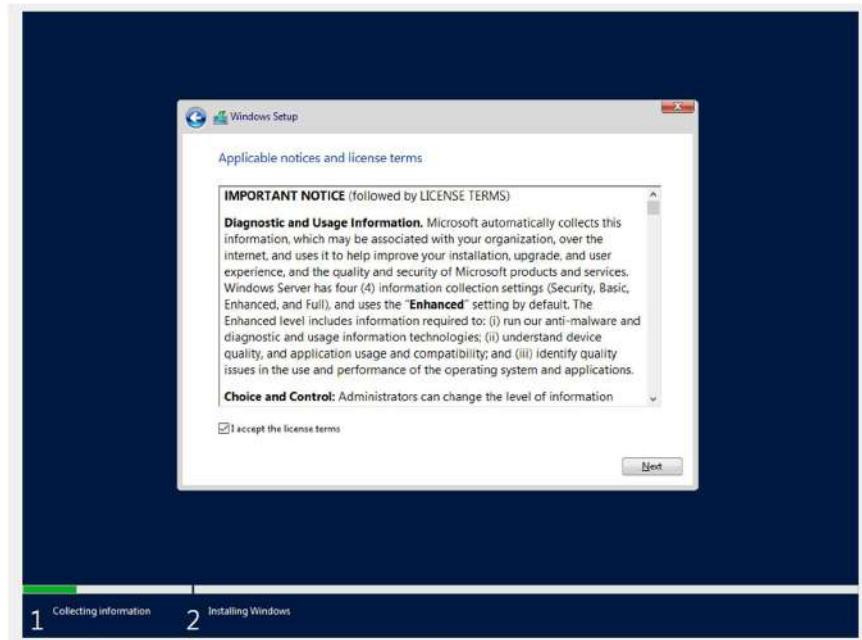
Click on **Install now**.



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

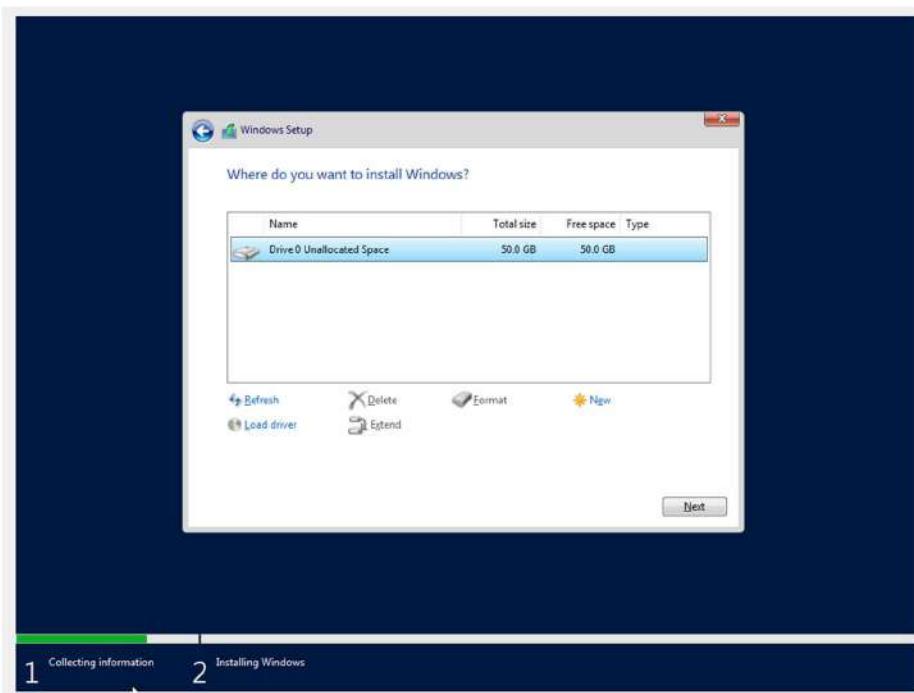


Accept the agreement and click on **Next**.

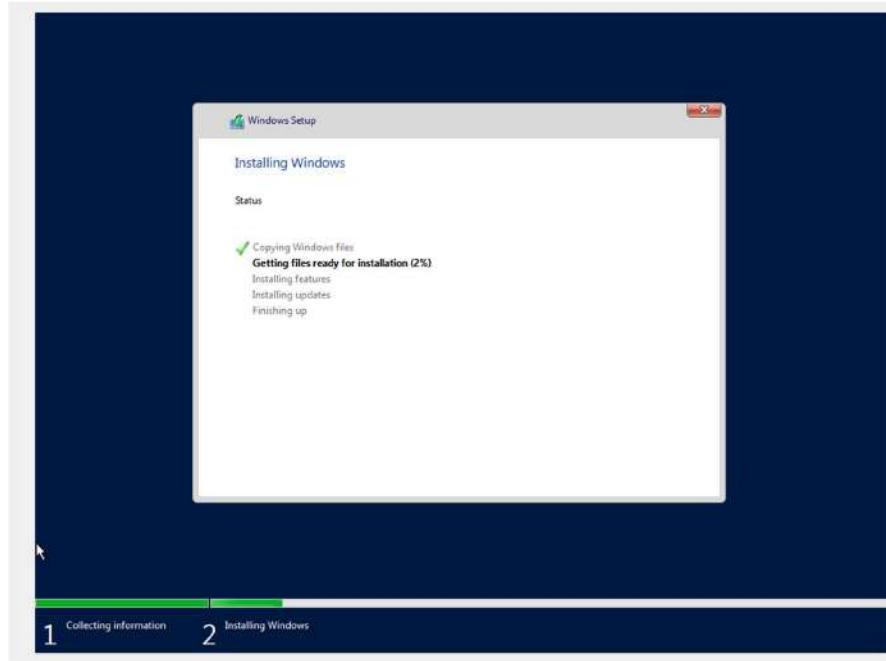


Select **Custom: Install Windows only (Advanced)**.

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

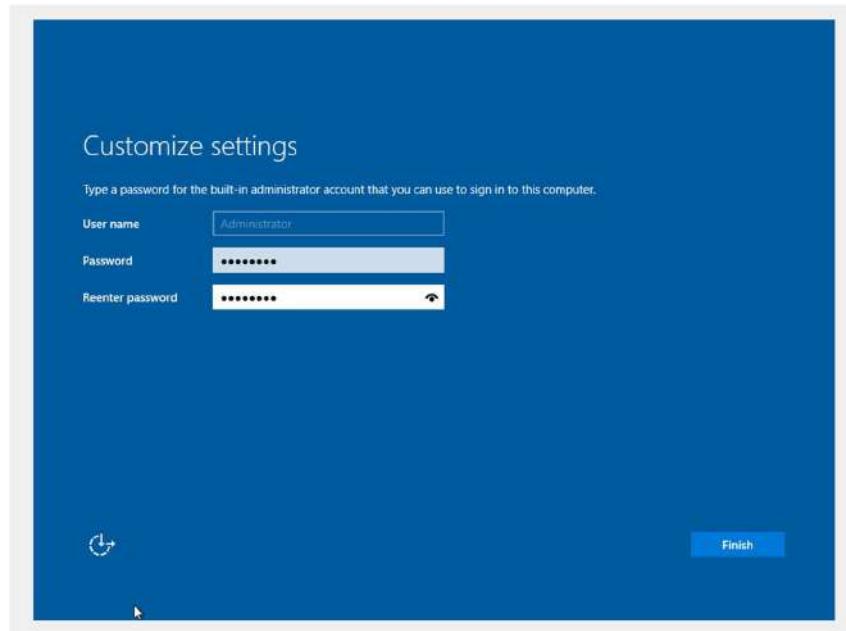


The VM will restart a couple of times during the installation process.

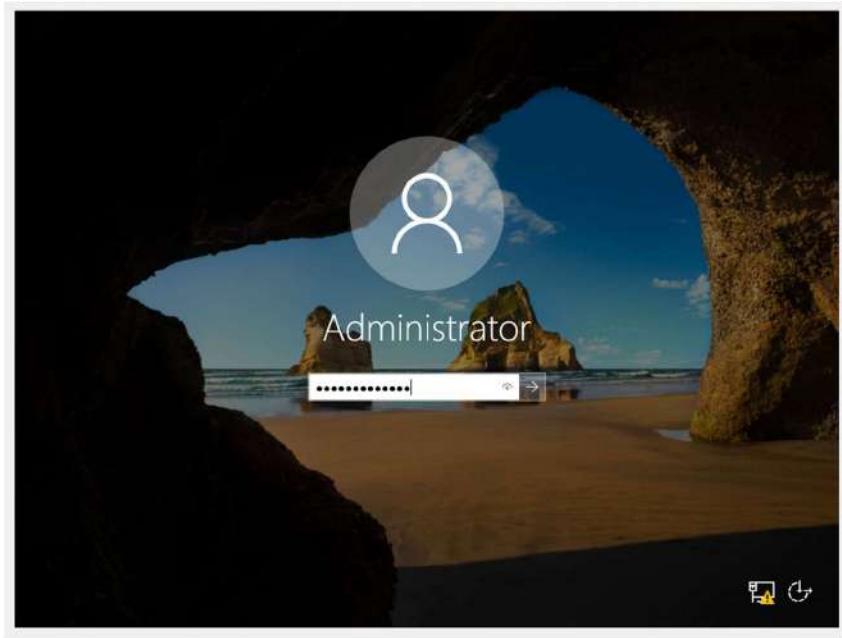


## OS Setup & Configuration

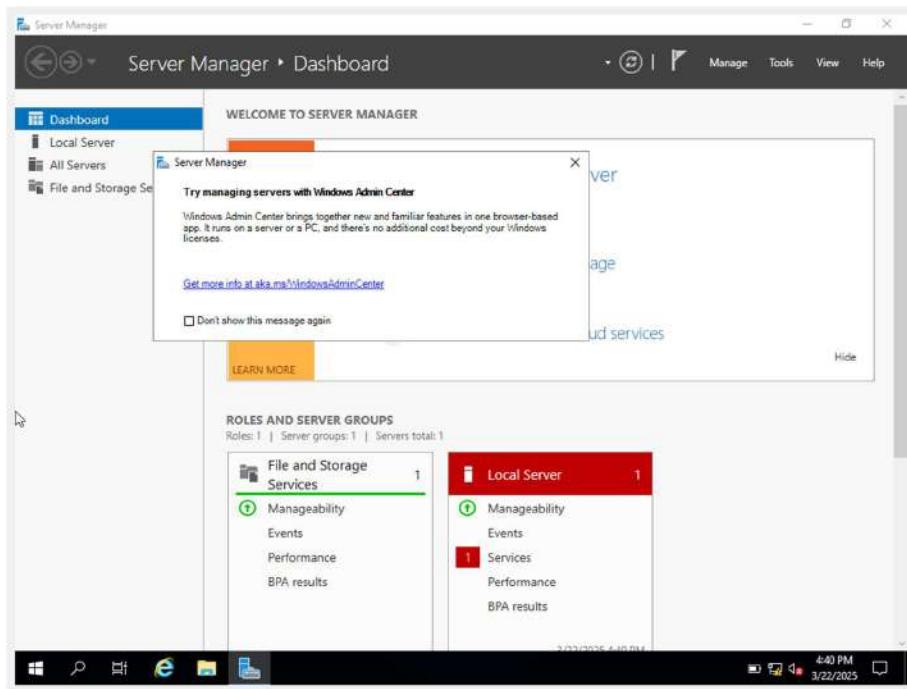
Once the installation is complete we will be asked to set the password for the Administrator account. Once set click on **Finish**.



For login press **ctrl + delete** button then password is asked

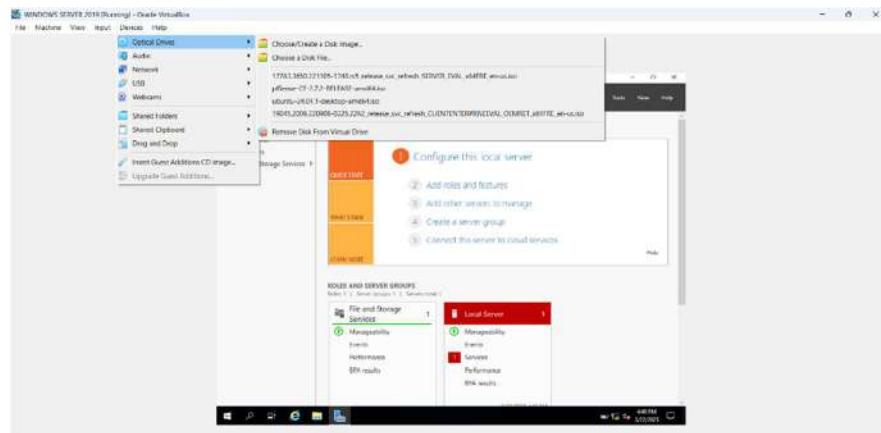


Once we log in, Server Manager will automatically open. A popup will also open asking us to try Windows Admin Center. Click on Don't show this message again and then click on X to close the popup.

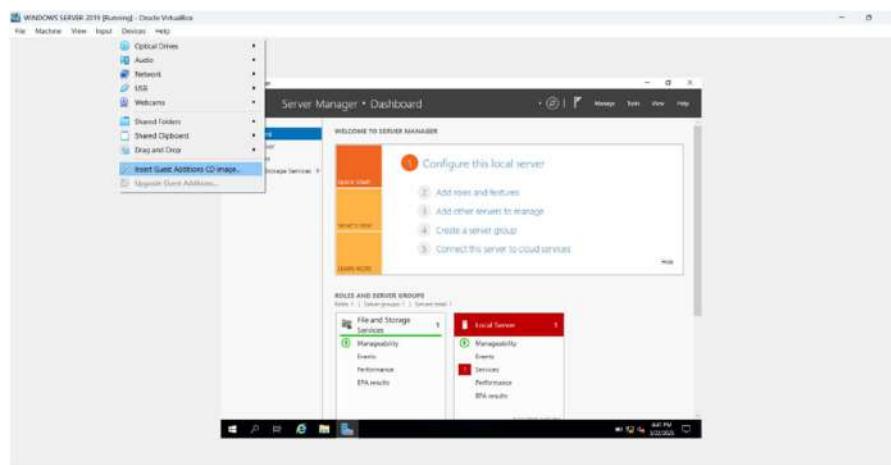


### Guest Additions Installation

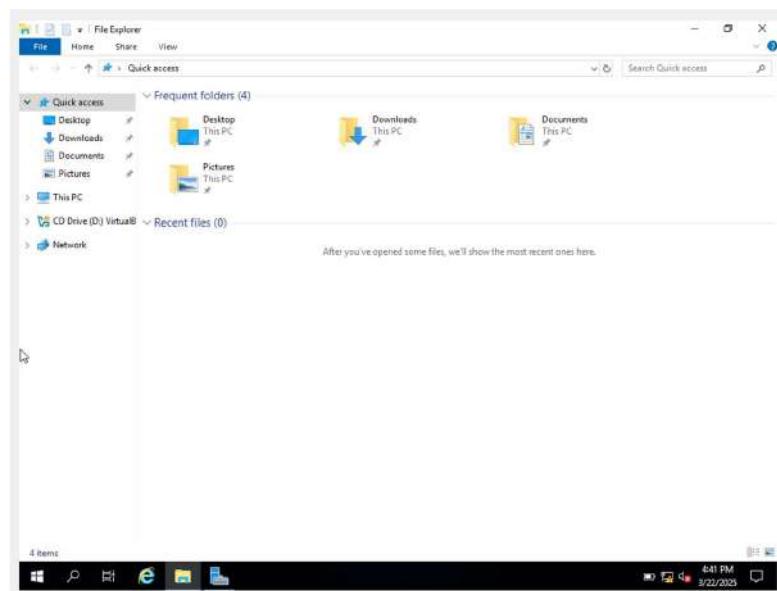
To make the VM screen size bigger we need to install Guest Additions. From the VM toolbar click on **Devices** -> **Optical Devices** -> **Remove disk from virtual drive**. This will remove the Windows Server 2019 image from the disk drive.



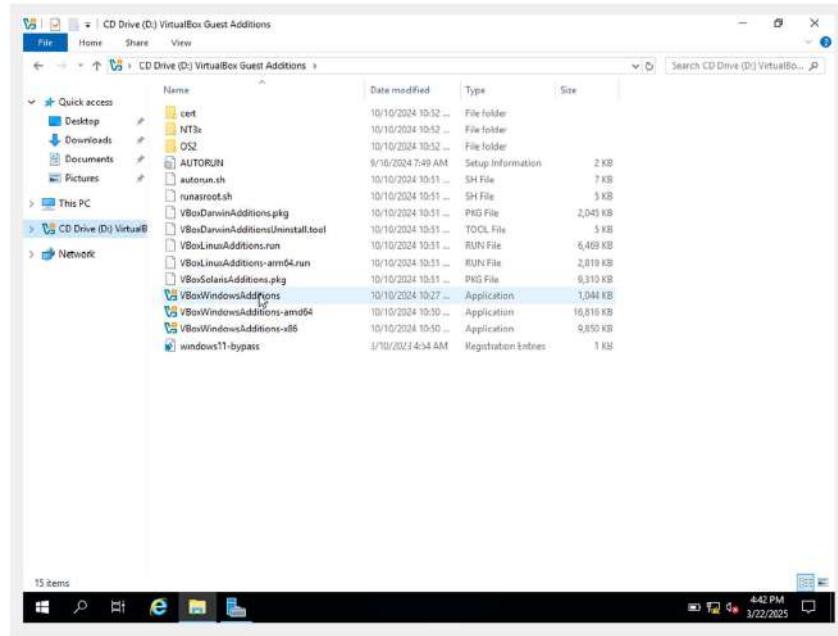
Then select **Devices** -> **Insert Guest Additions CD image**.



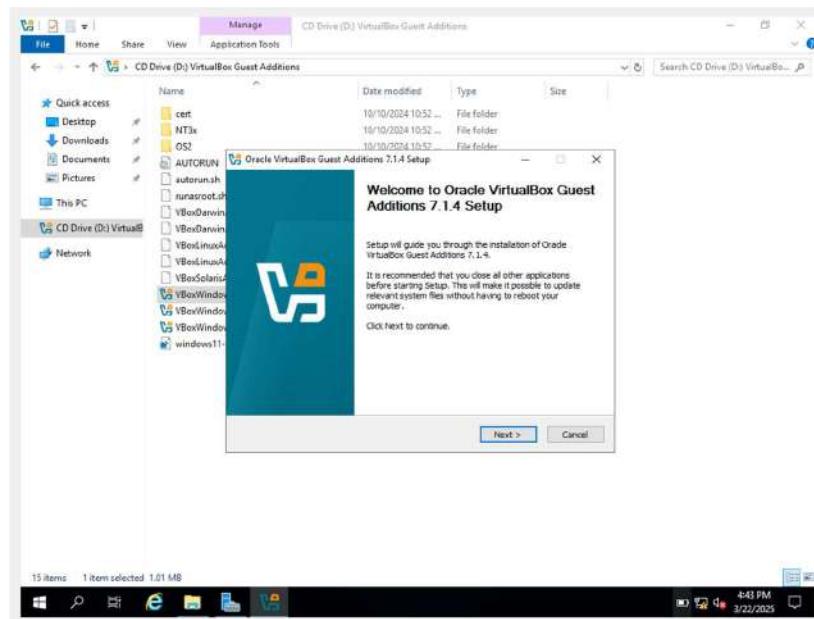
Open file explorer then **CD Drive** option shows click on it



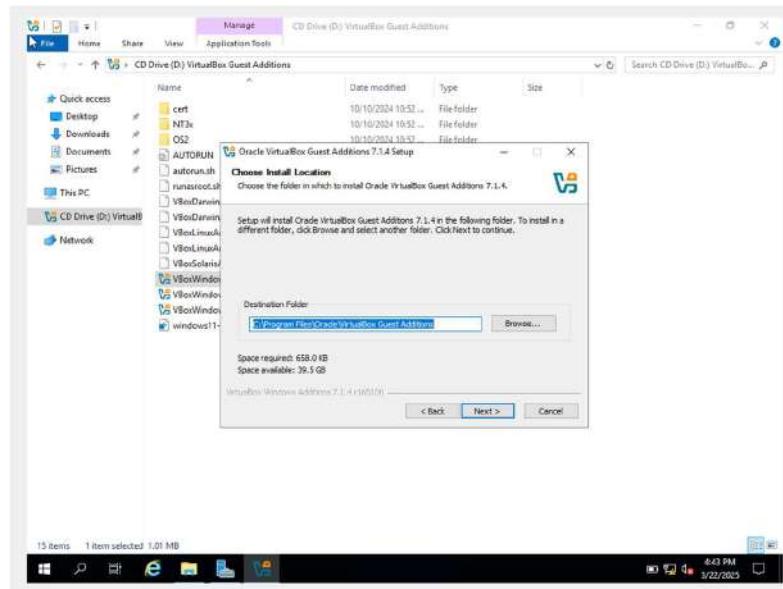
Double-click on **VboxWindowsAdditions** (4<sup>th</sup> file from bottom) to start the installer.



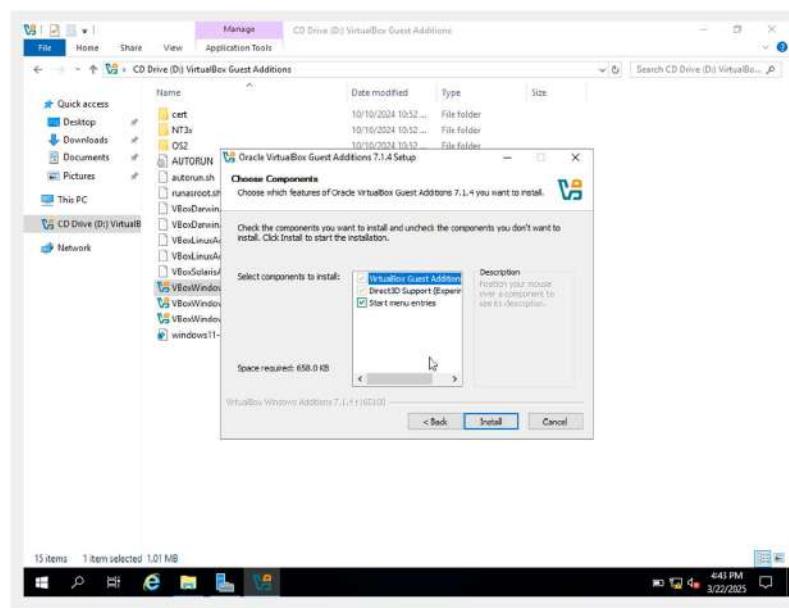
Click on Next.



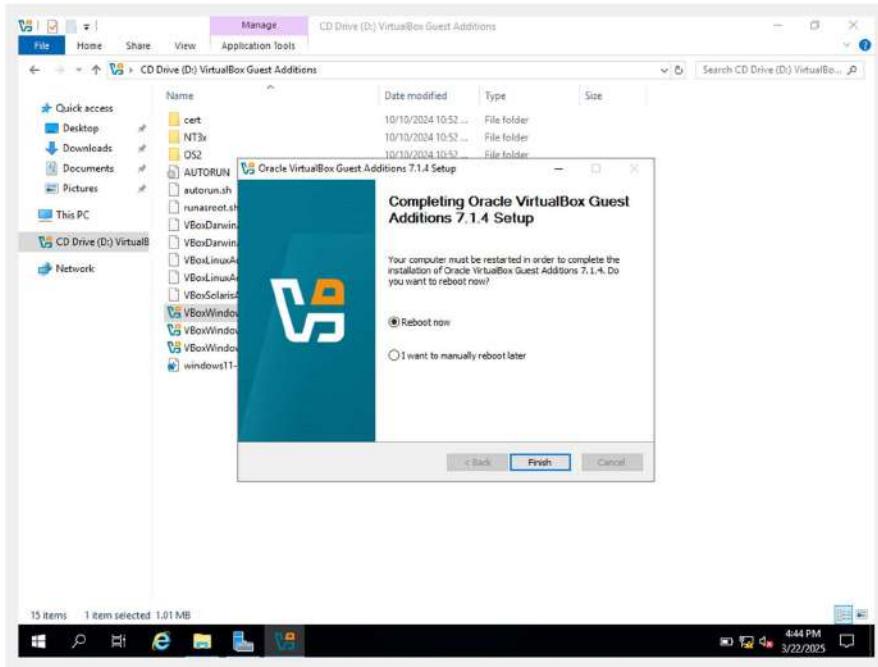
Click on Next.



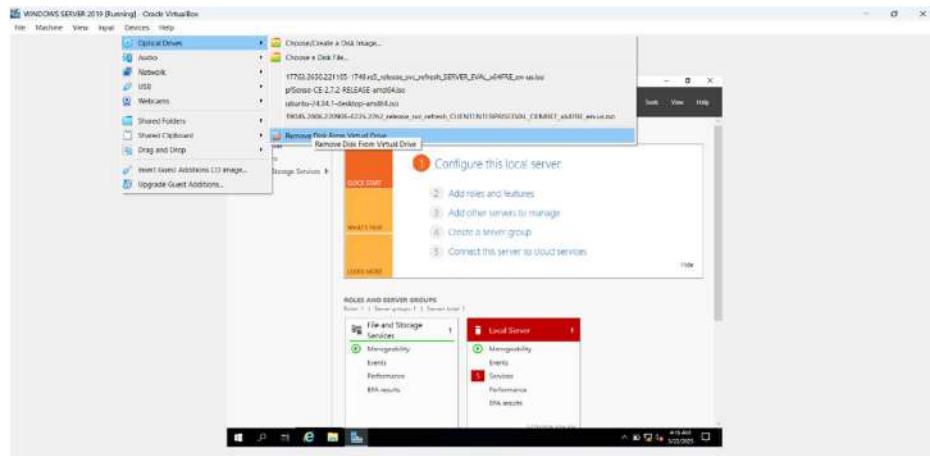
Click on **INSTALL**. For installing the requirement components.



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



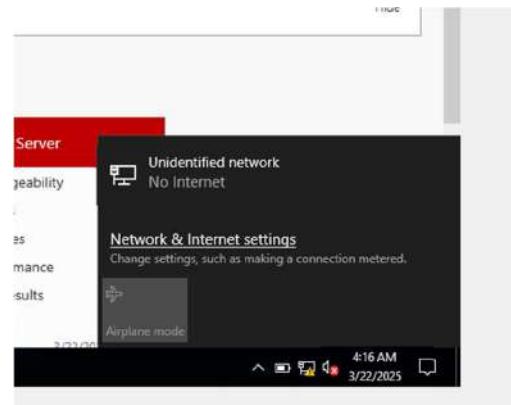
After restart, log into the system. From the VM toolbar click on **Devices -> Optical Drivers -> Remove disk from virtual drive** to remove the Guest Additions image



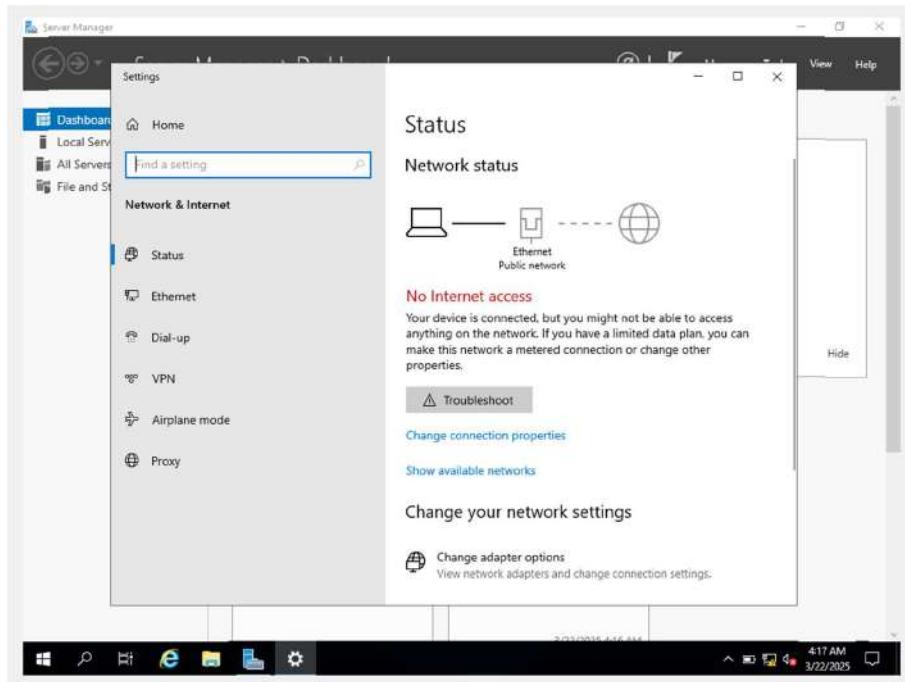
Use the shortcut **Right Ctrl+F** to enter Fullscreen mode. The VM will automatically scale to fill the entire screen. Use the same shortcut to exit Fullscreen mode.

### Network Configuration

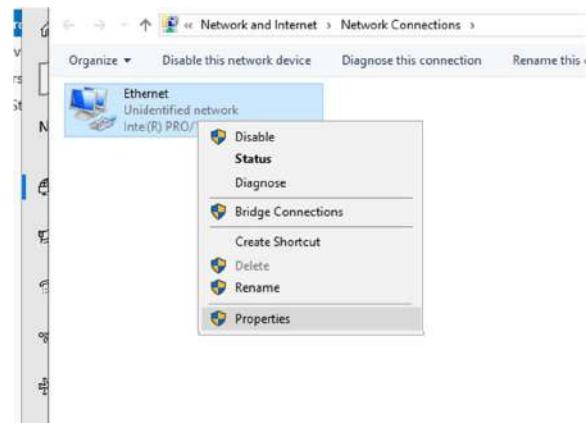
During the pfSense setup module we disabled DHCP on the **AD\_LAB** interface because of this our VM will not be automatically assigned an IP address. From the taskbar right-click on the network icon and select **Open Network & Internet settings**.



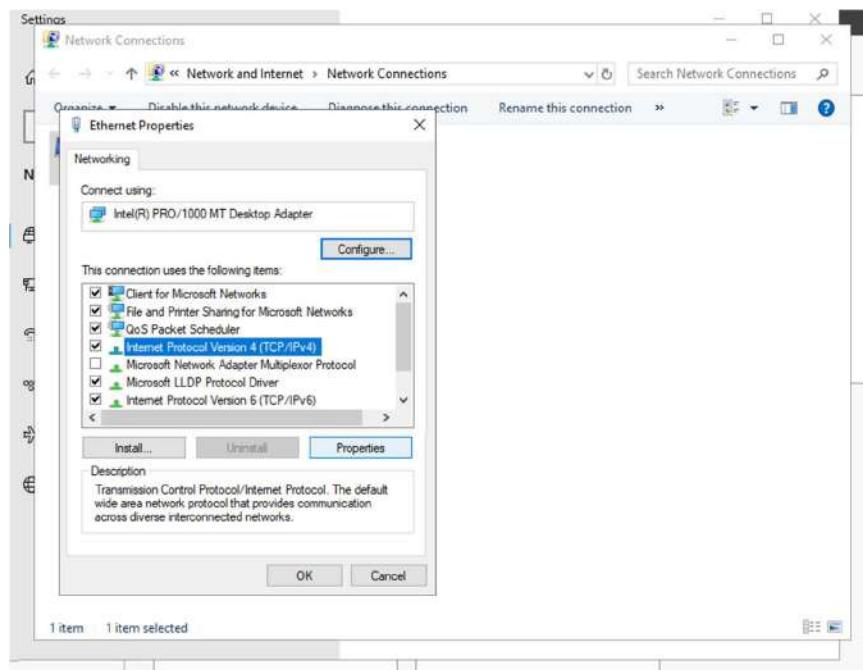
Click on “Change adapter options”.



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**.



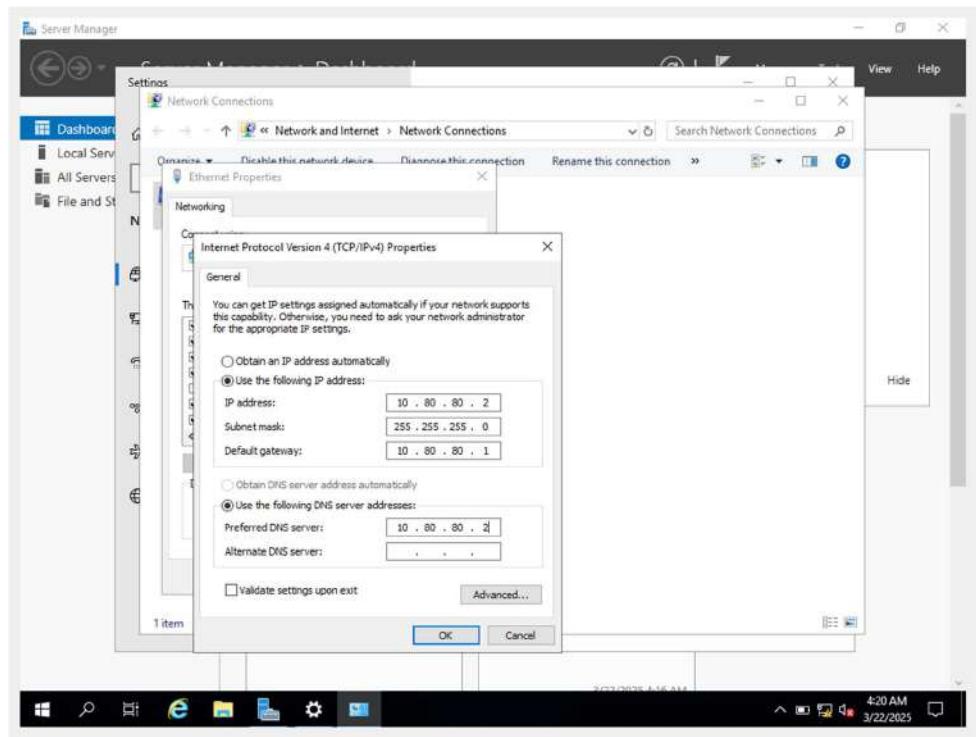
Enter the details as shown below and then click on **OK**. Click on **OK** again to close the Ethernet Properties menu.

IP address: **10.80.80.2**

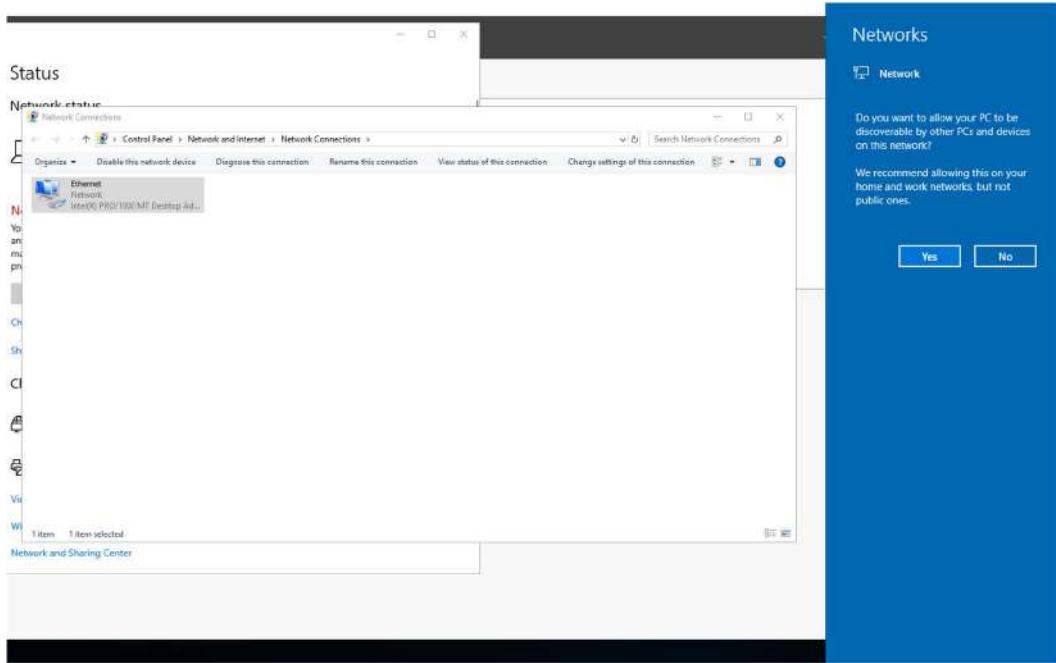
Subnet mask: **255.255.255.0**

Default gateway: **10.80.80.1**

Preferred DNS Server: **10.80.80.2**

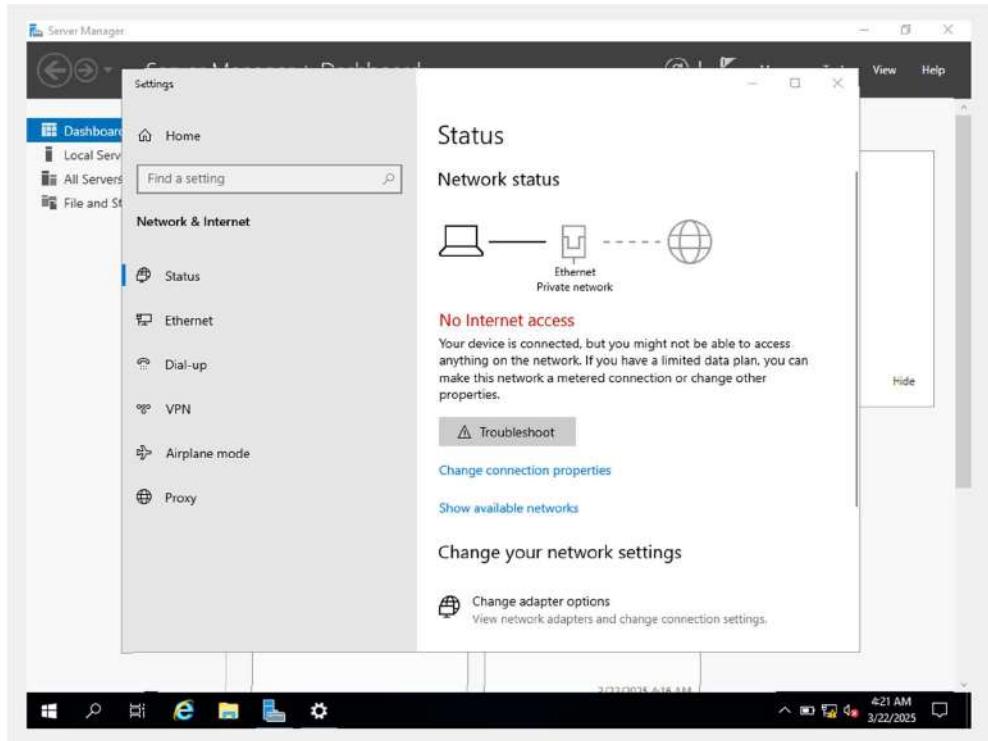


Windows will display a banner to allow internet access click on **Yes**.



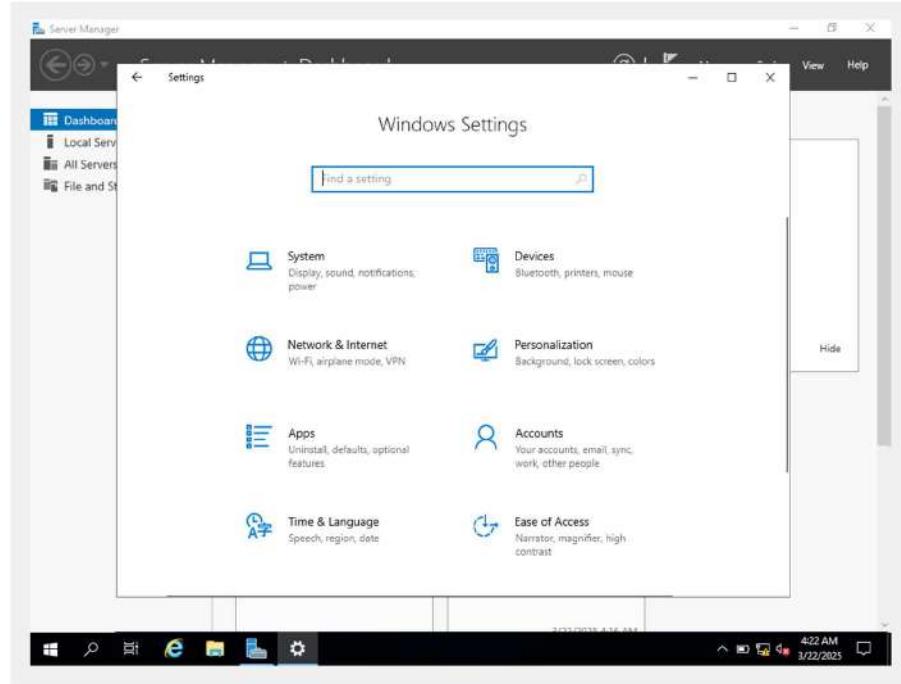
Close the Network Connections page.

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

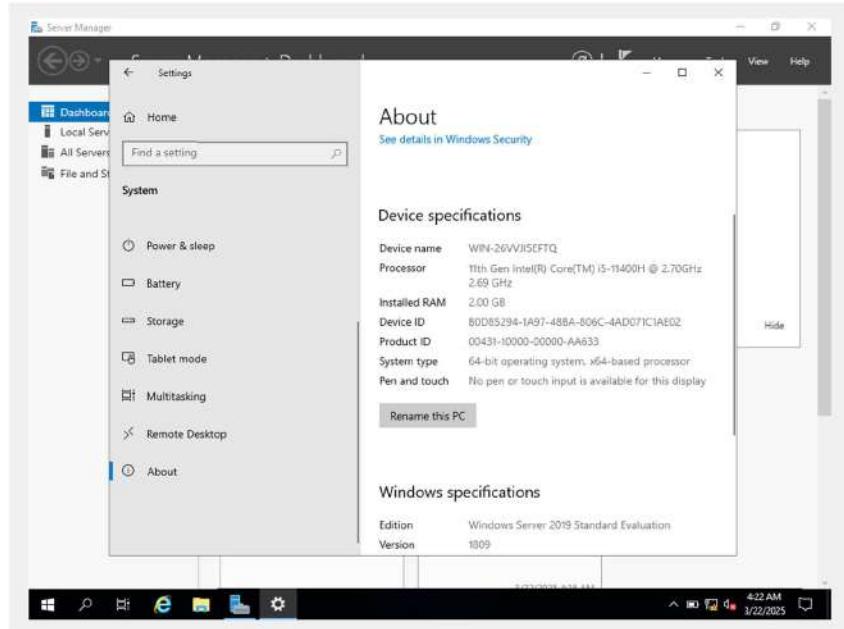


## Renaming the System

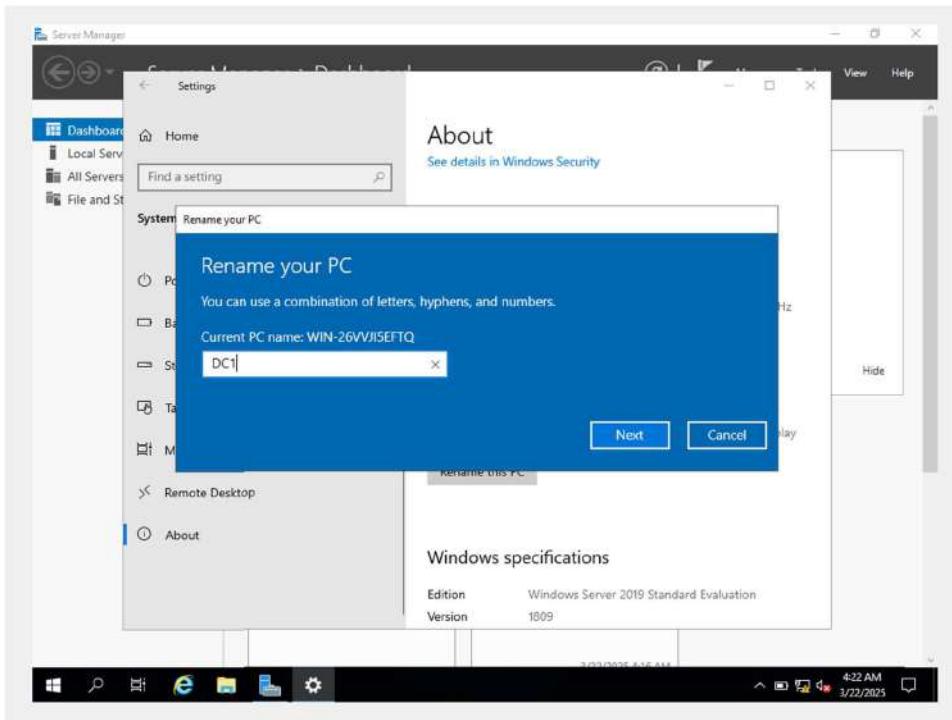
Before we can set up the machine to be a Domain Controller let us rename the PC. Select “System”.



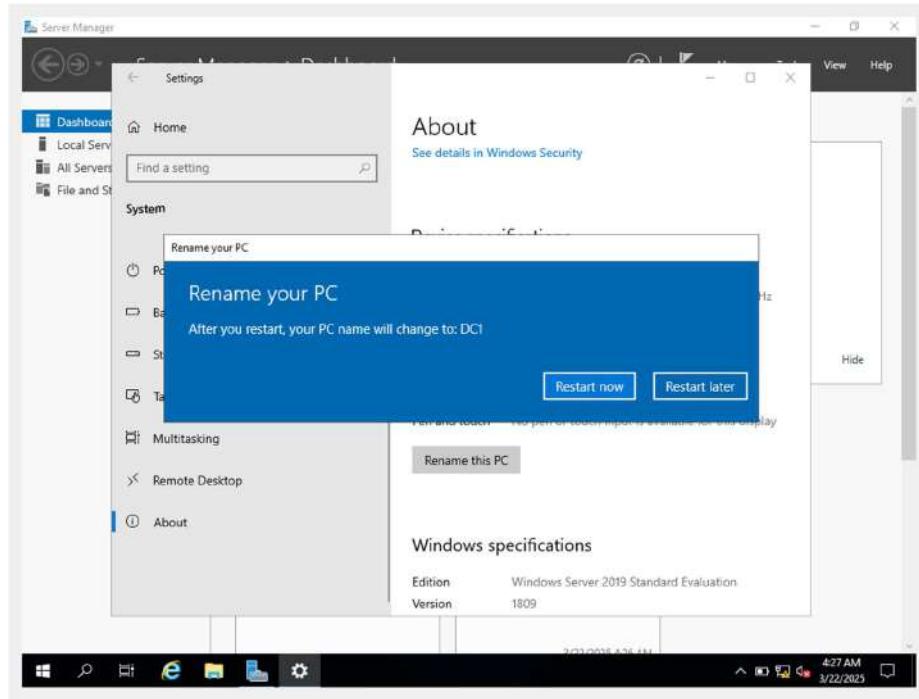
Click on About on the sidebar and then click on the “Rename this PC” button.



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

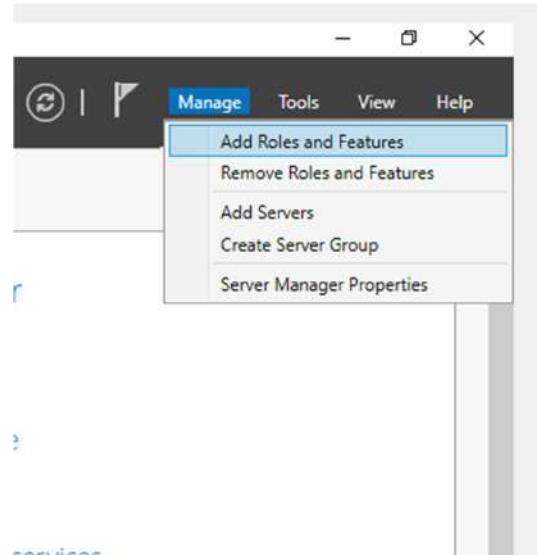


Click on “Restart now” for the changes to take effect.

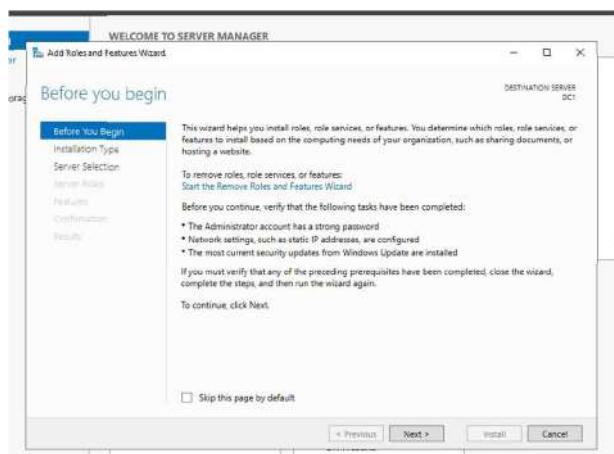


## Active Directory & DNS Installation

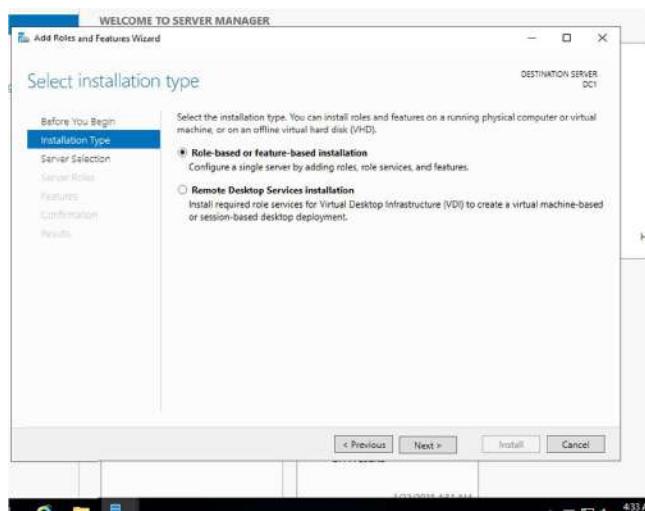
After login wait for Server Manager to load. Click on the **Manage** button from the top right corner and select “Add Roles and Features”.



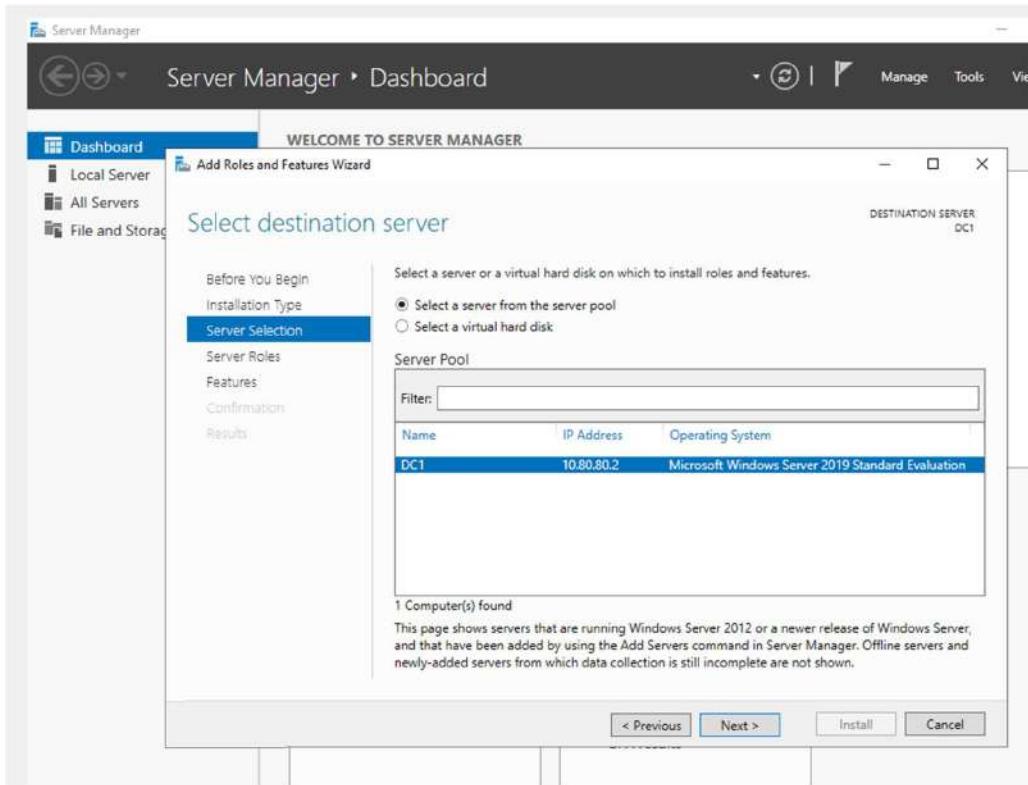
Click on **Next**



Click on **Next**

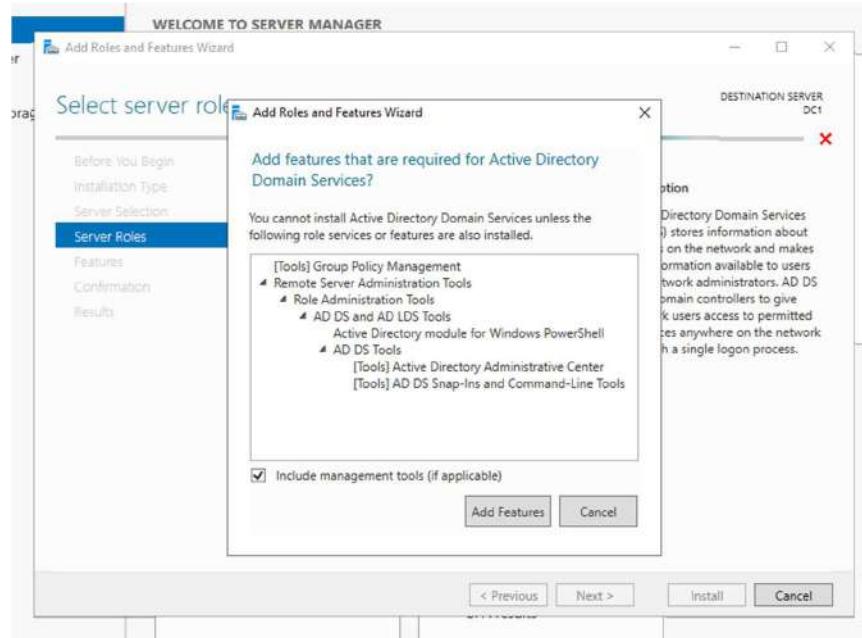


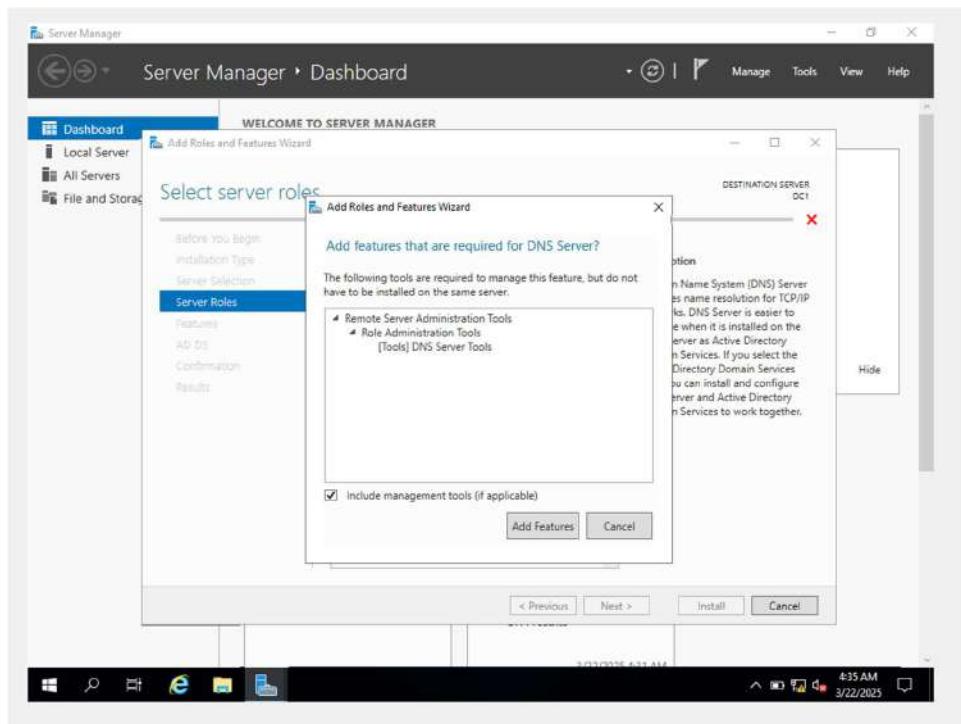
Click on Next



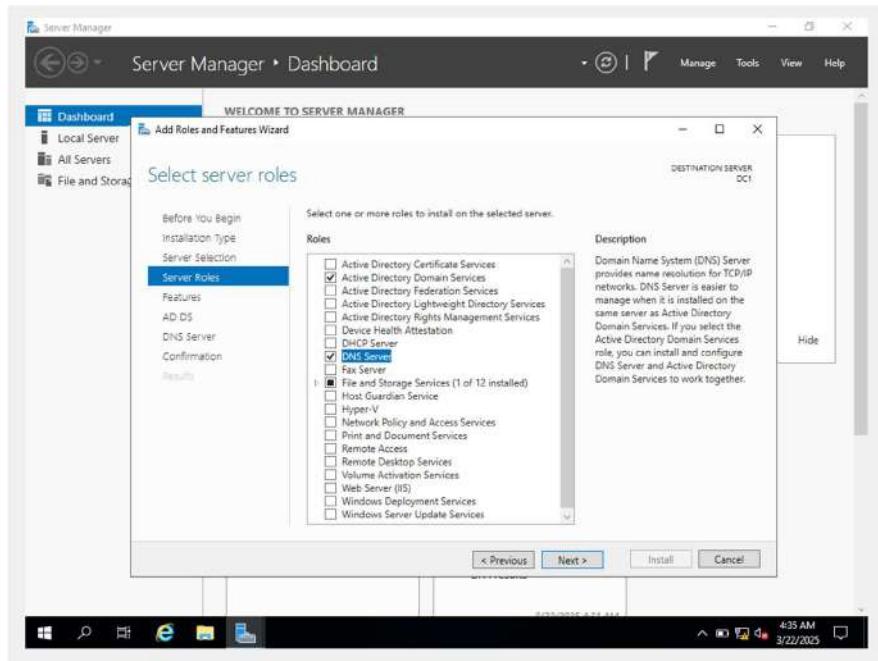
On this page enable “Active Directory Domain Services” and “DNS Server”.

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

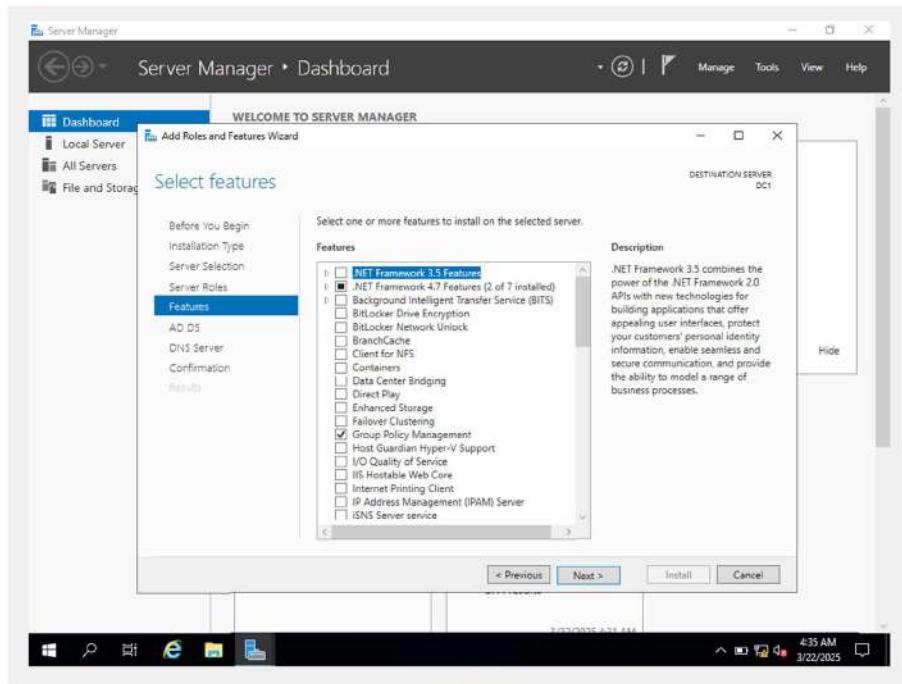




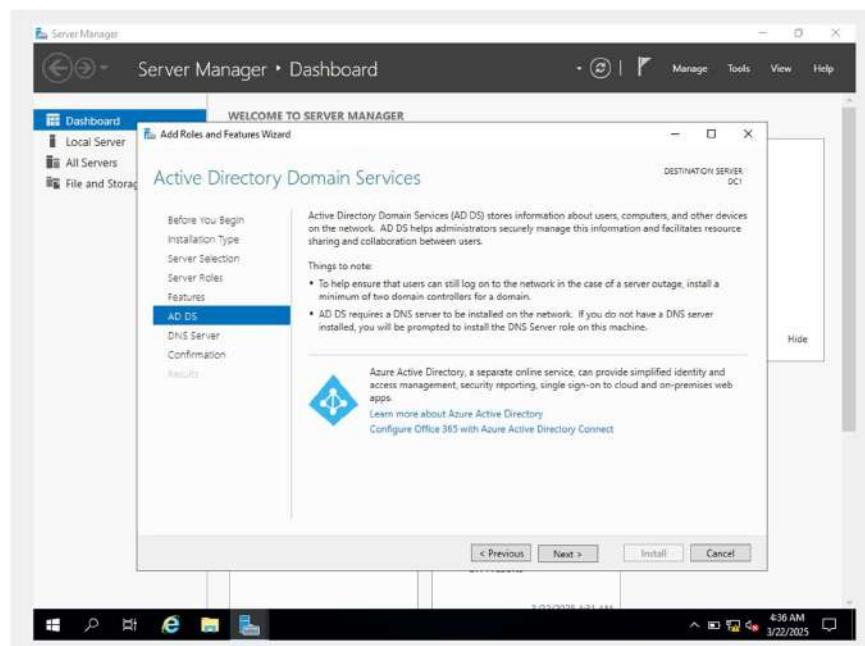
Once both the features are selected click on **Next** to proceed with installation.



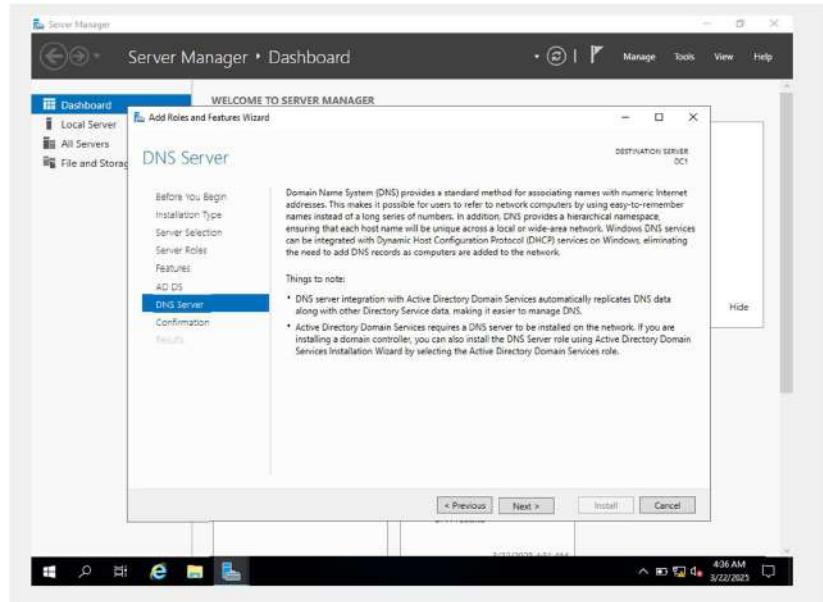
Click on **Next**



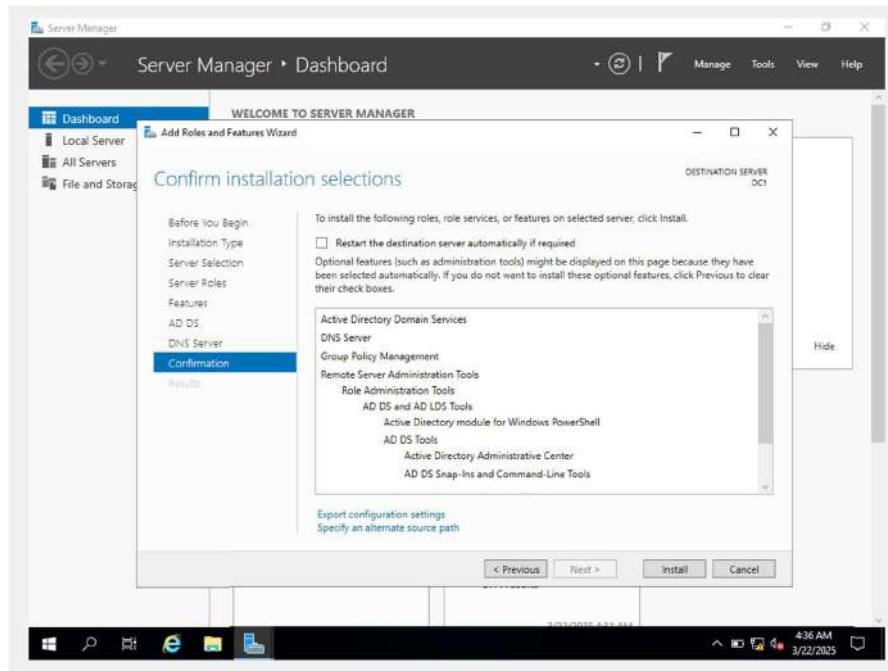
Click on Next



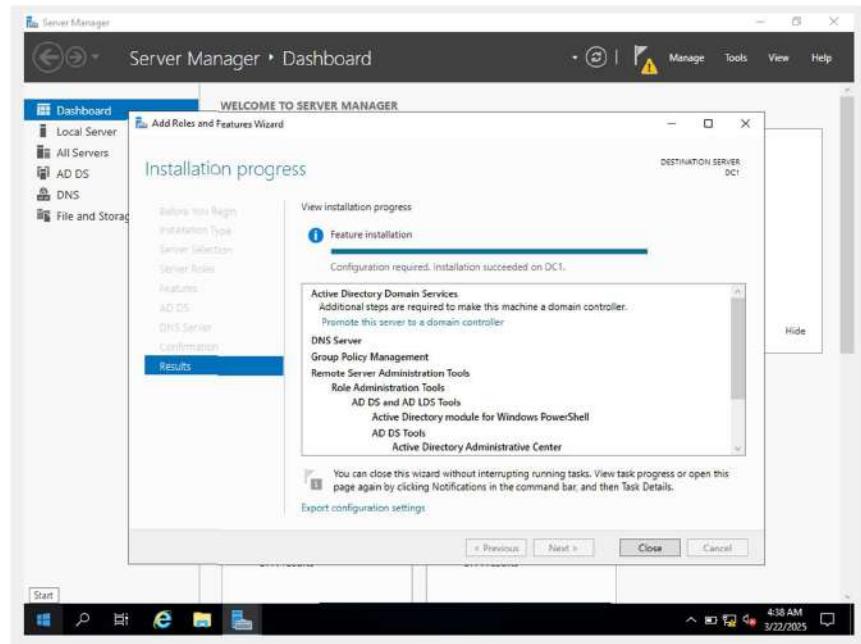
Click on Next



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

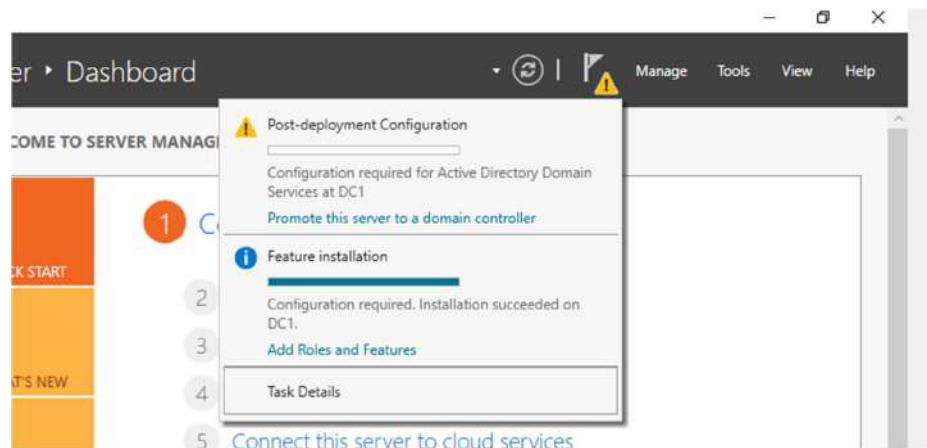


Once the installation is complete click on **Close** to exit the Wizard.

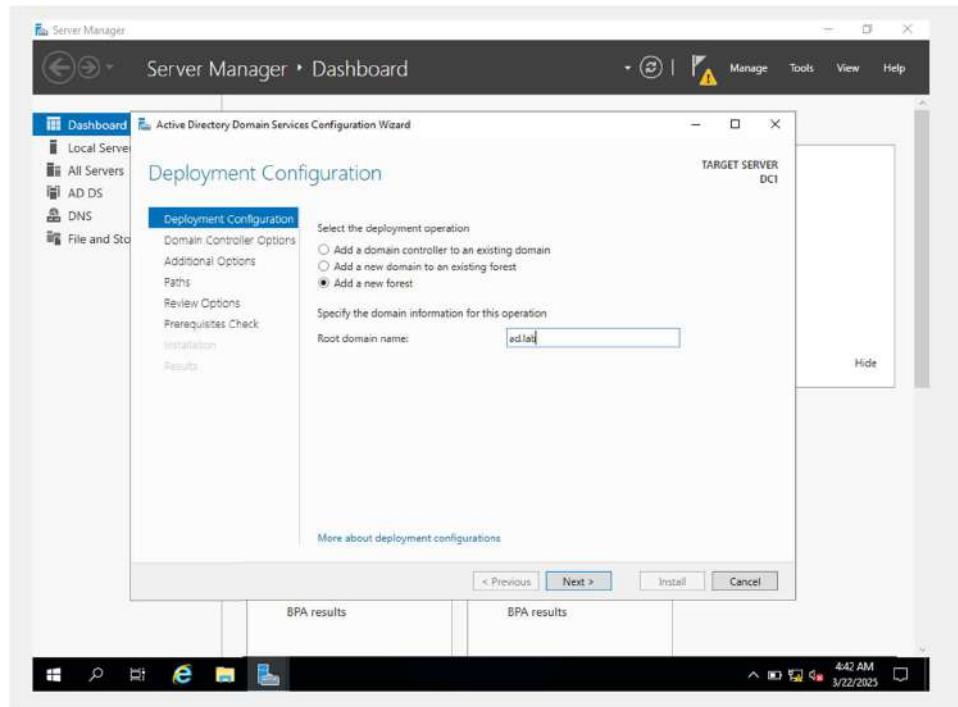


## Active Directory Configuration

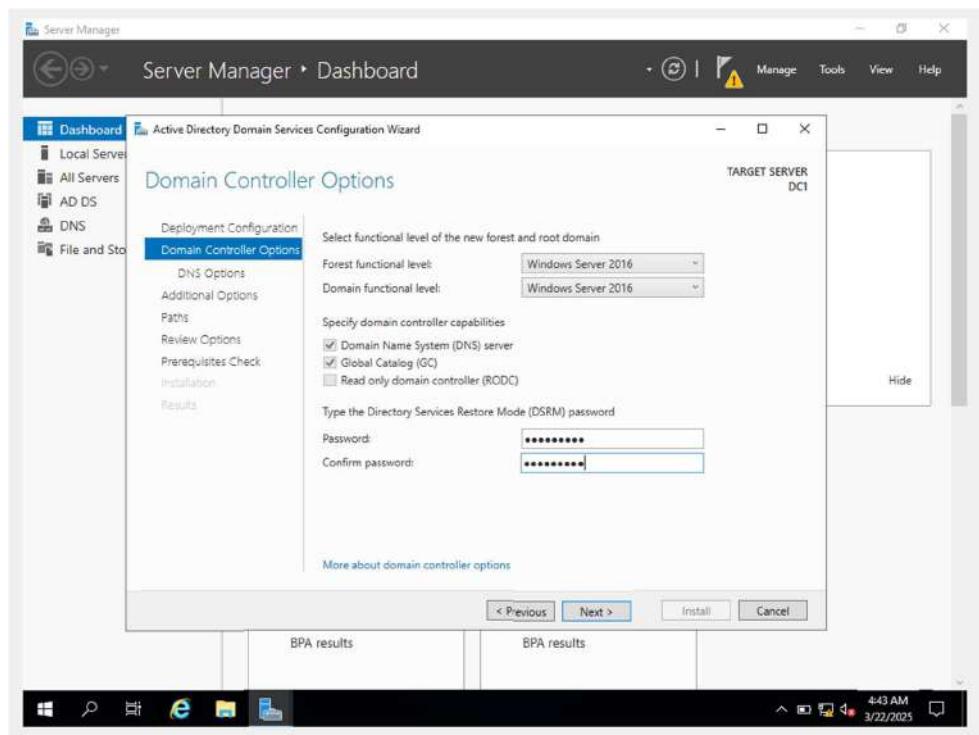
Click on the Flag icon present in the top right of the toolbar in Server Manager. From the dropdown click on “Promote this server to a domain controller”.



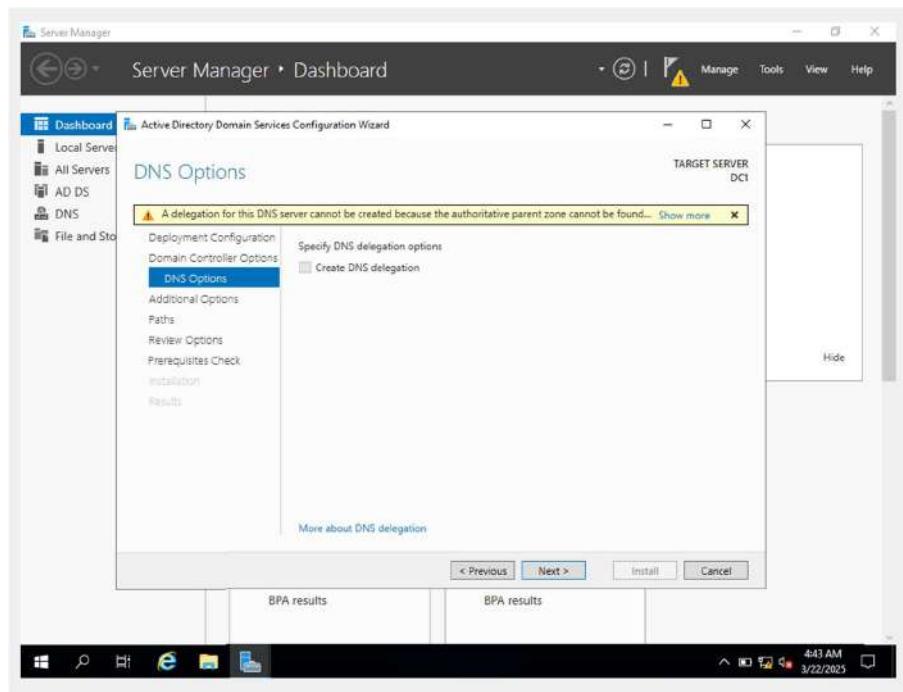
The AD Domain Servers Configuration Wizard will open. For deployment operation select **Add a new Forest**. Give the domain a name. For my setup, I will be using the domain name **ad.lab**. After selecting the name click on **Next**.



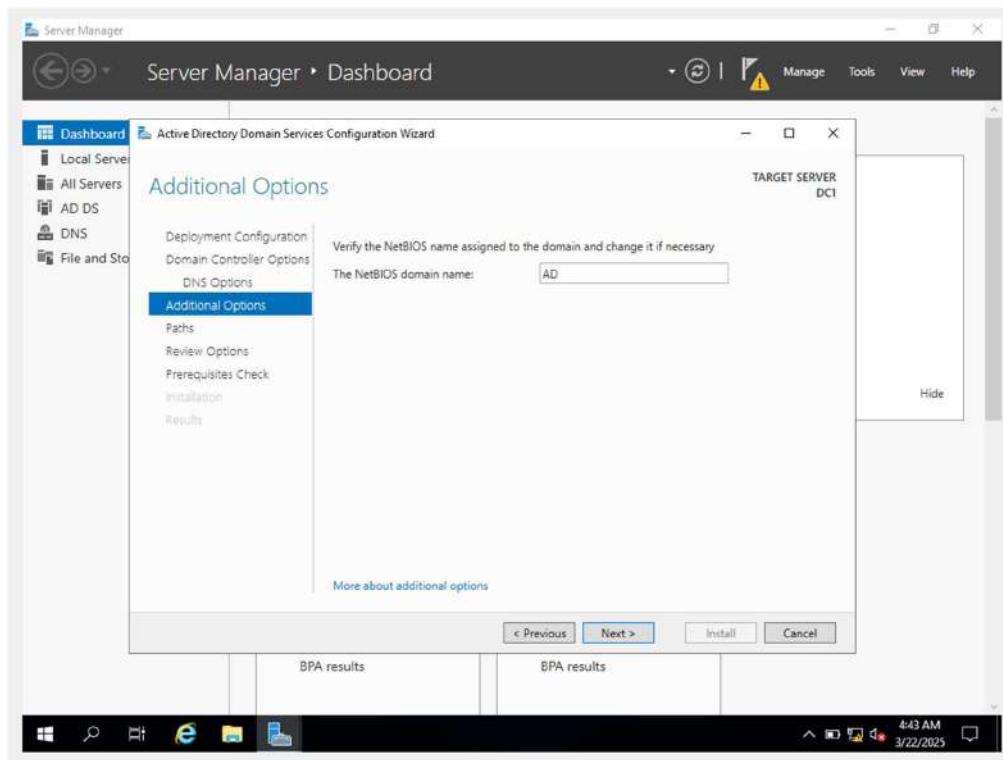
On this page enter a password to use for using the AD Restore feature.



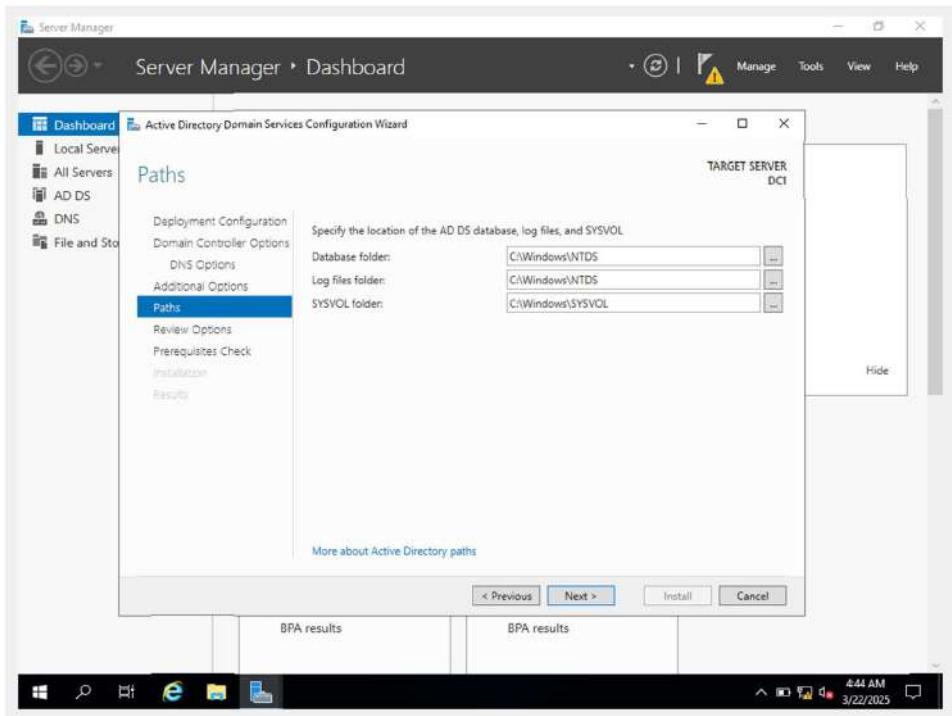
Ignore the warning that is shown and click on **Next**.



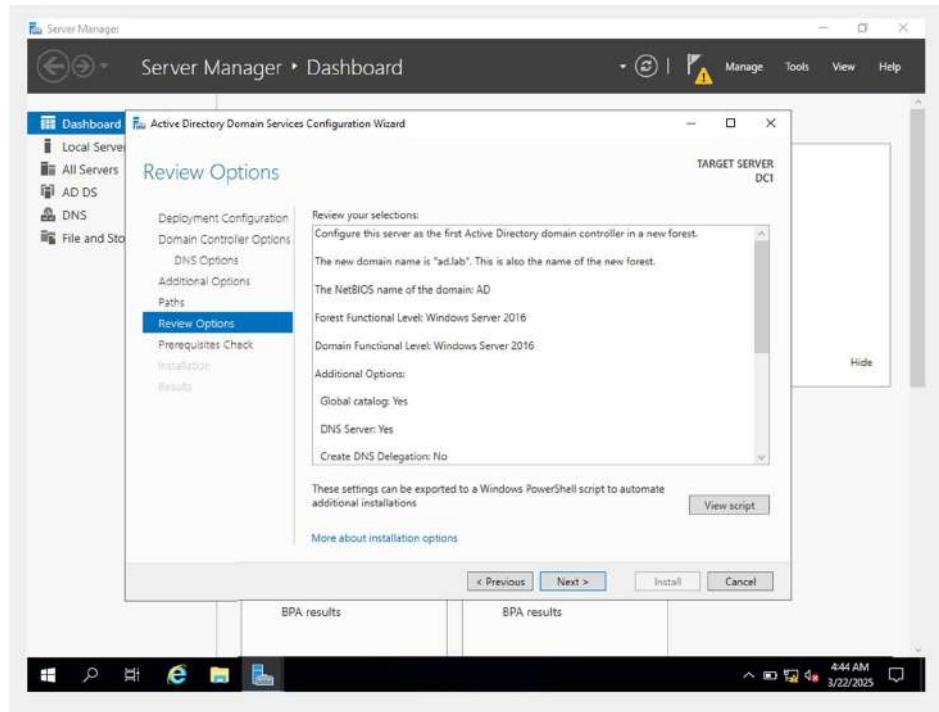
The NetBIOS name should automatically be filled. It will be the first part of the domain name. Click on **Next** to continue.



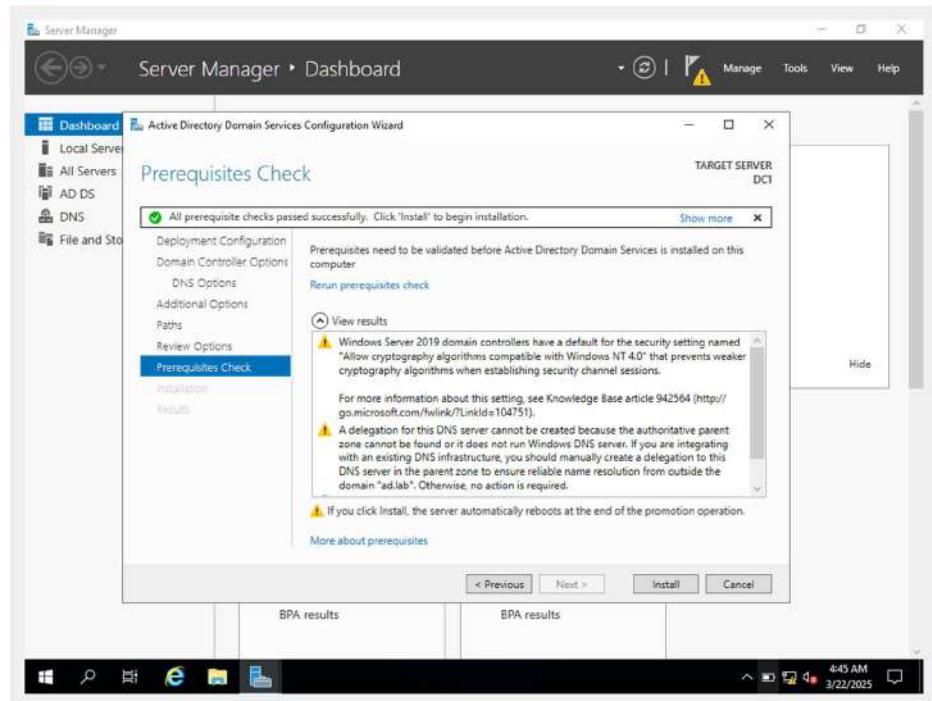
Click on **Next**.



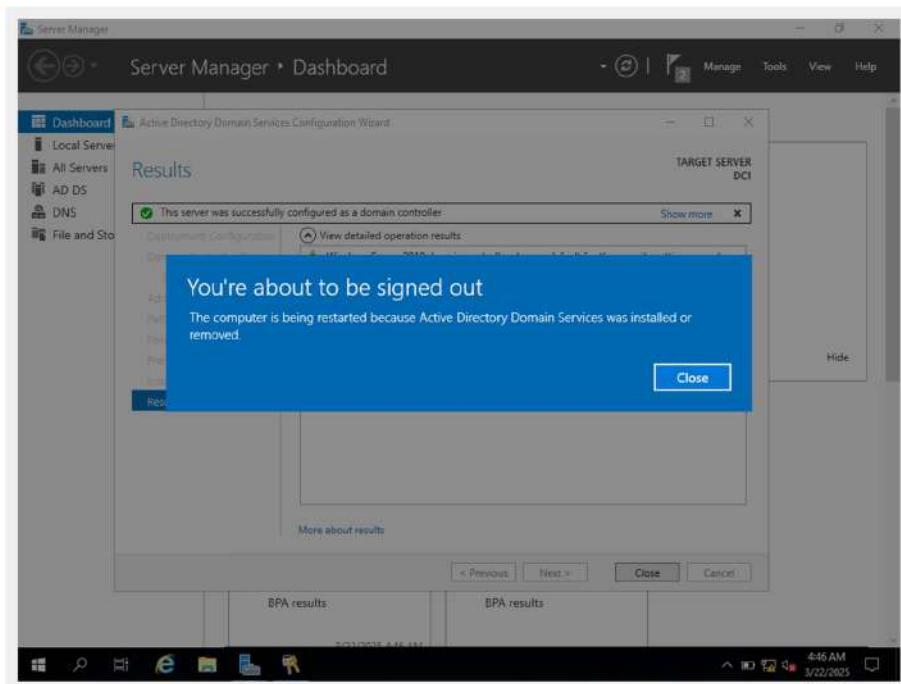
Click on **Next**.



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.

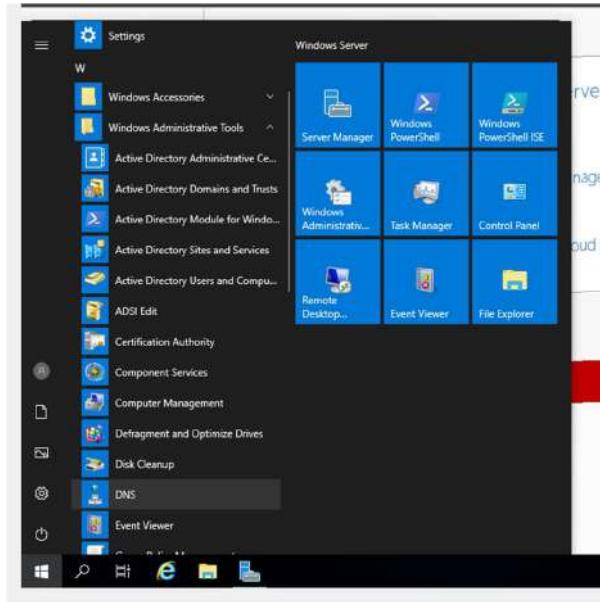


On restart, you will notice that the name that is shown on the login page has changed. The first part of the domain name is prepended to the username. This means the machine has successfully been configured as the domain controller. Log in using the Administrator password.

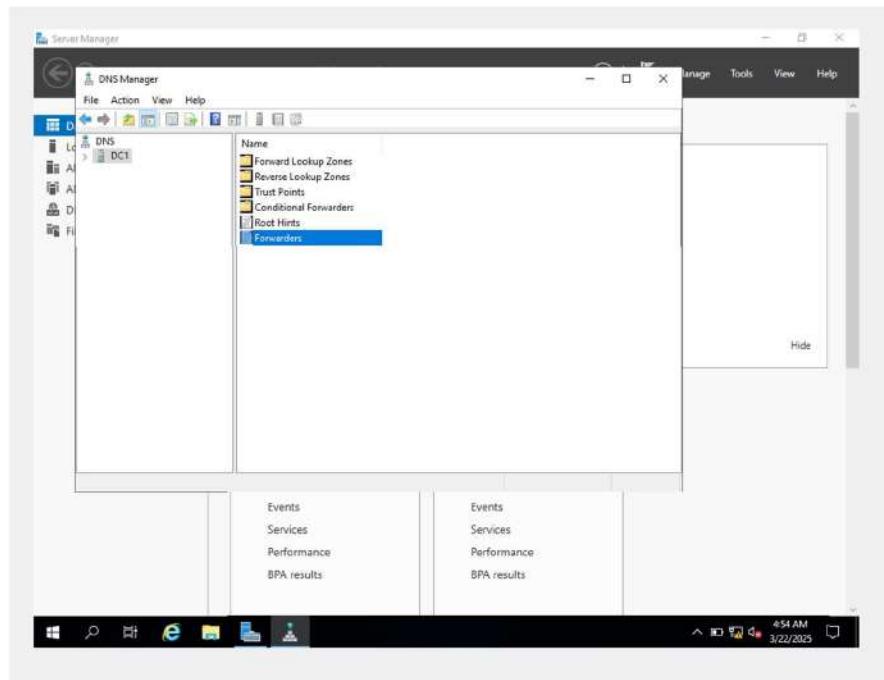
## DNS Configuration

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.

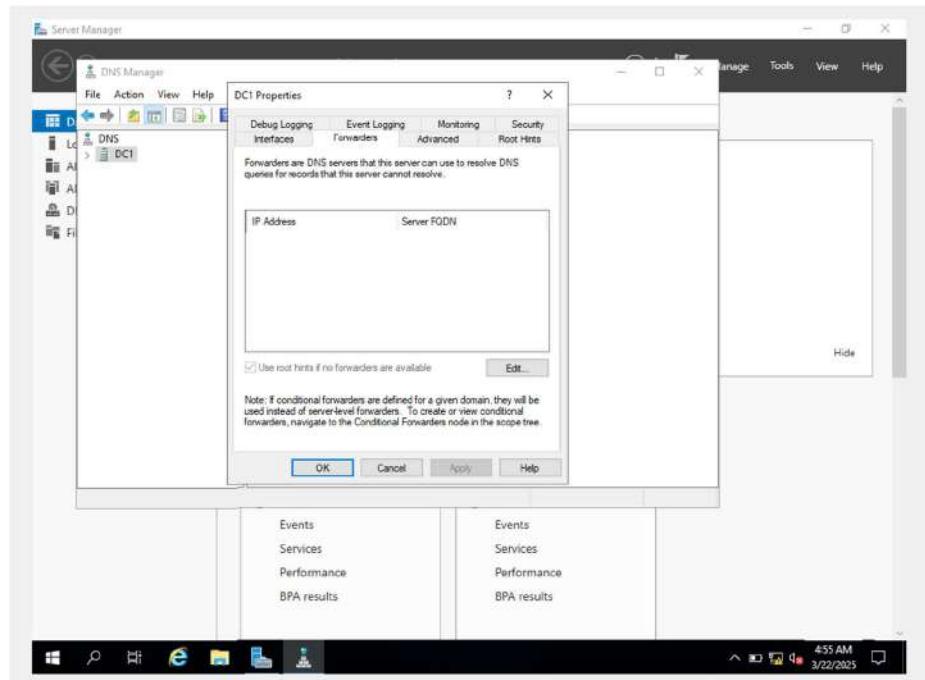
Open the Start menu expand the “Windows Administrative Tools” folder and select **DNS**.



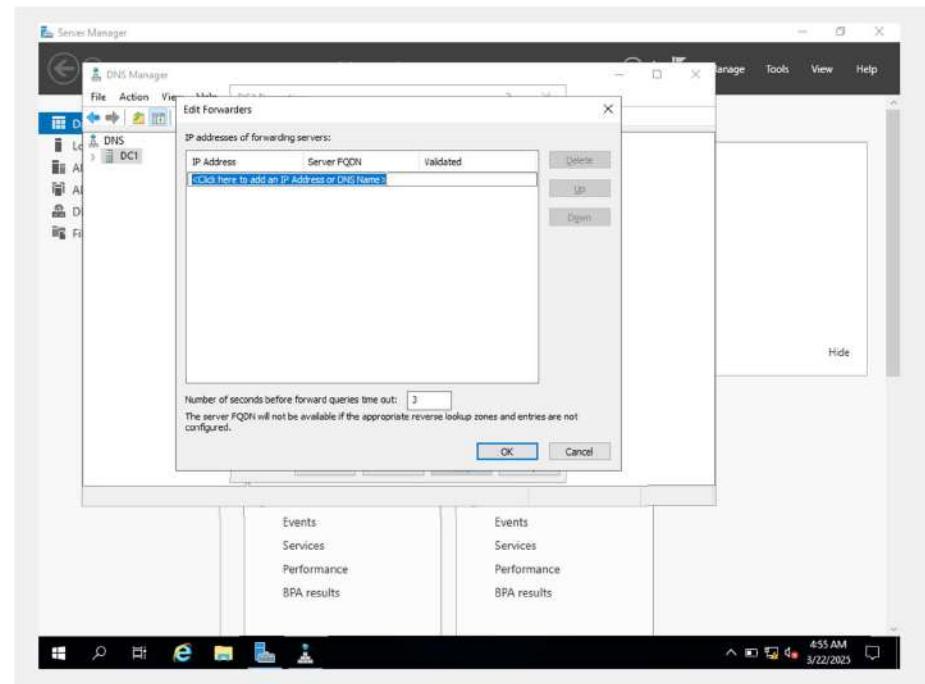
In the sidebar select the Domain Controller (in my case DC1) and from the right menu double-click on “Forwarders”.



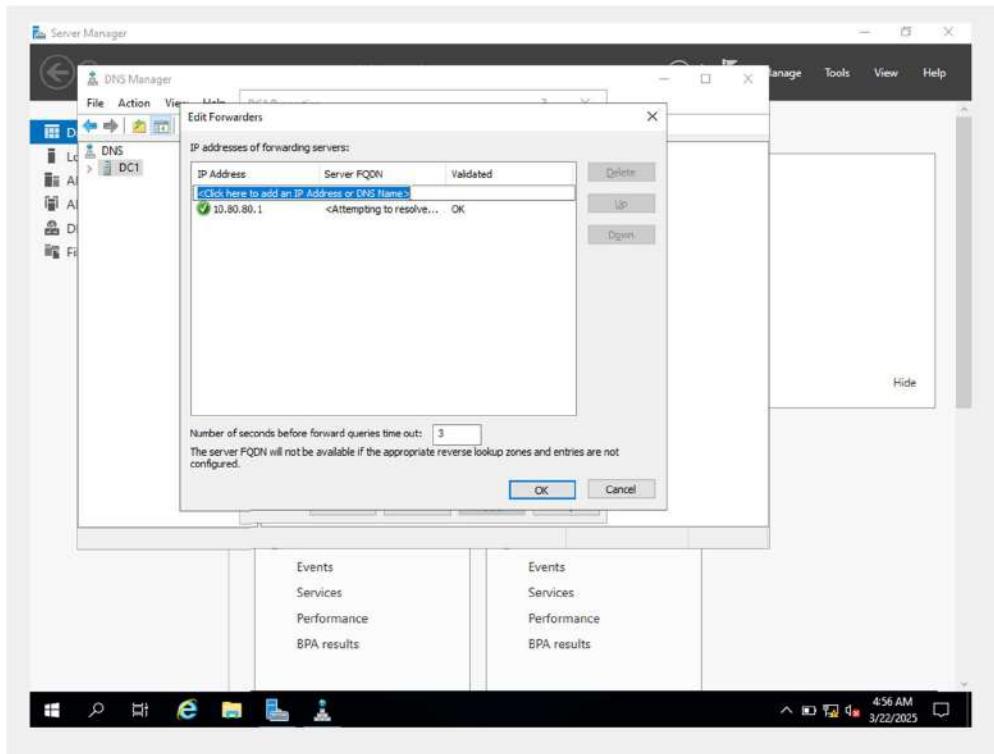
Go to **Forwarders** -> **Edit**.



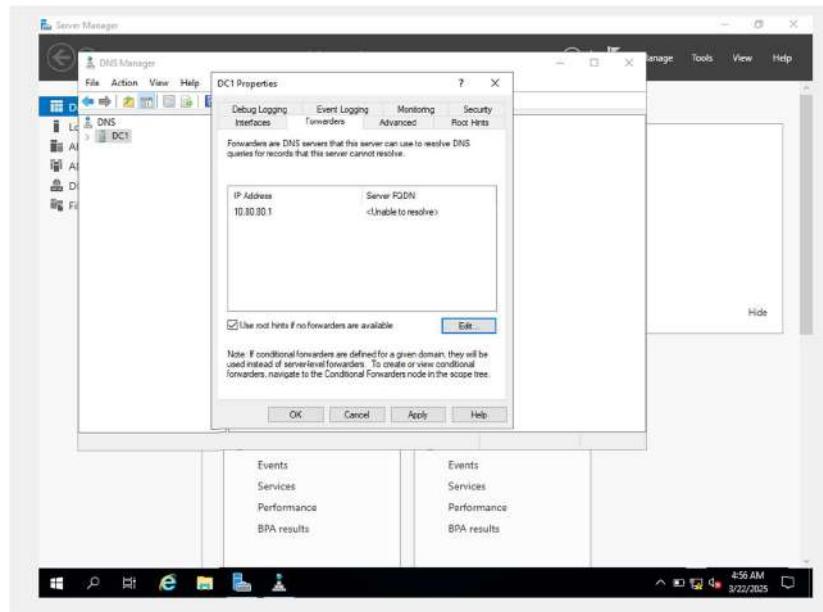
This will open the Forwarder configuration page. Enter the IP address of the **AD\_LAB** interface (**10.80.80.1**) and press **Enter**.



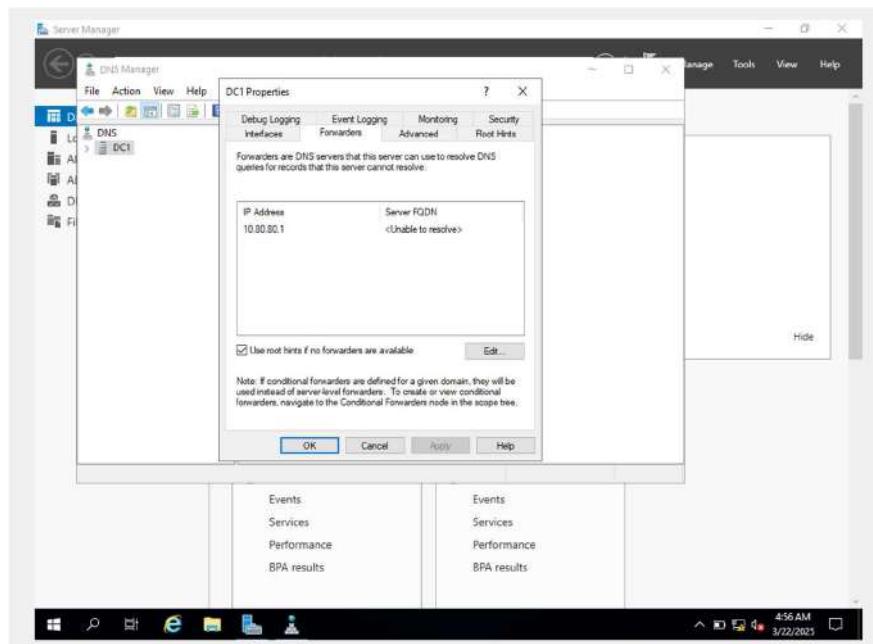
Once added. Click on **OK** to confirm the change.



Click on **Apply** .



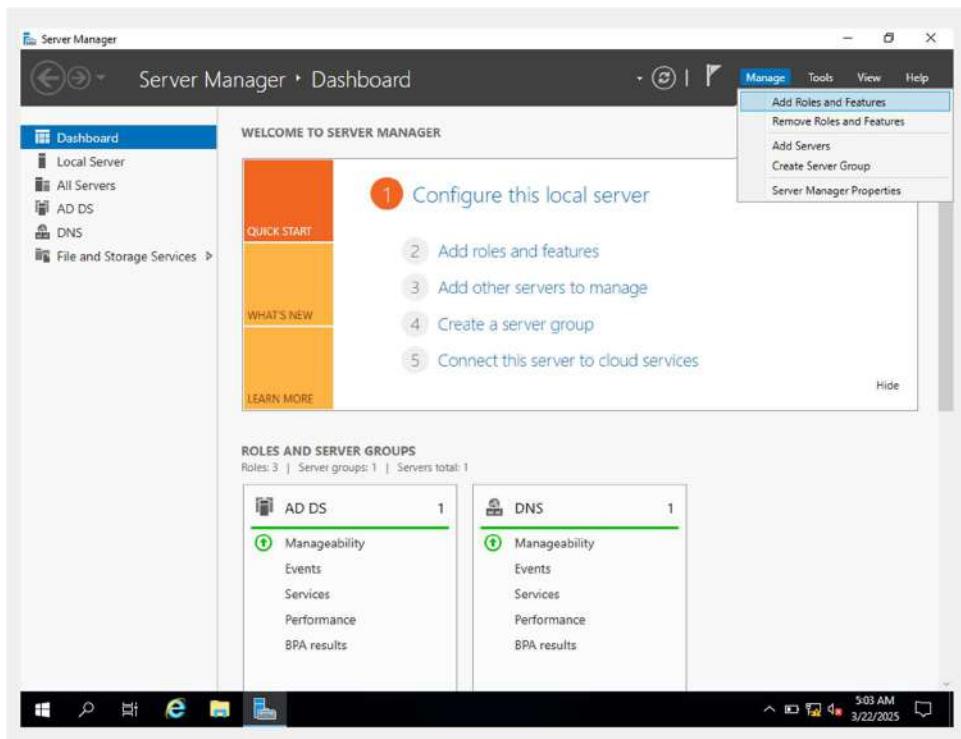
then **OK** to save the changes.



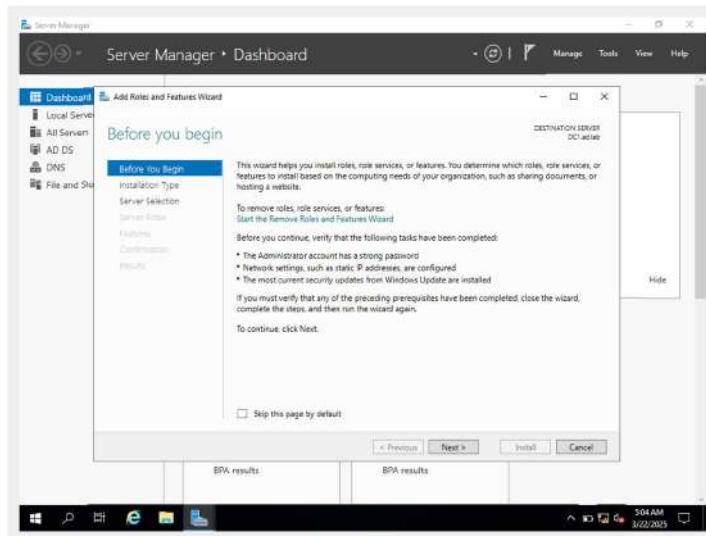
## DHCP Installation

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.

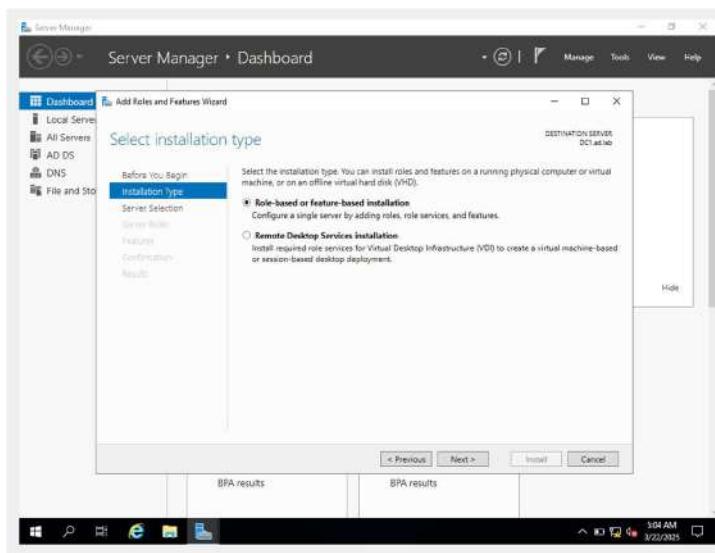
Click on Manage from the toolbar in Server Manager. Then choose “Add Roles and Features”.



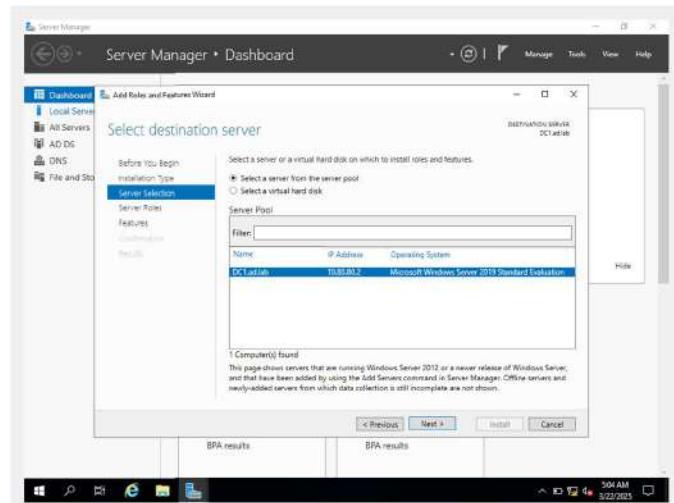
Click on **Next**.



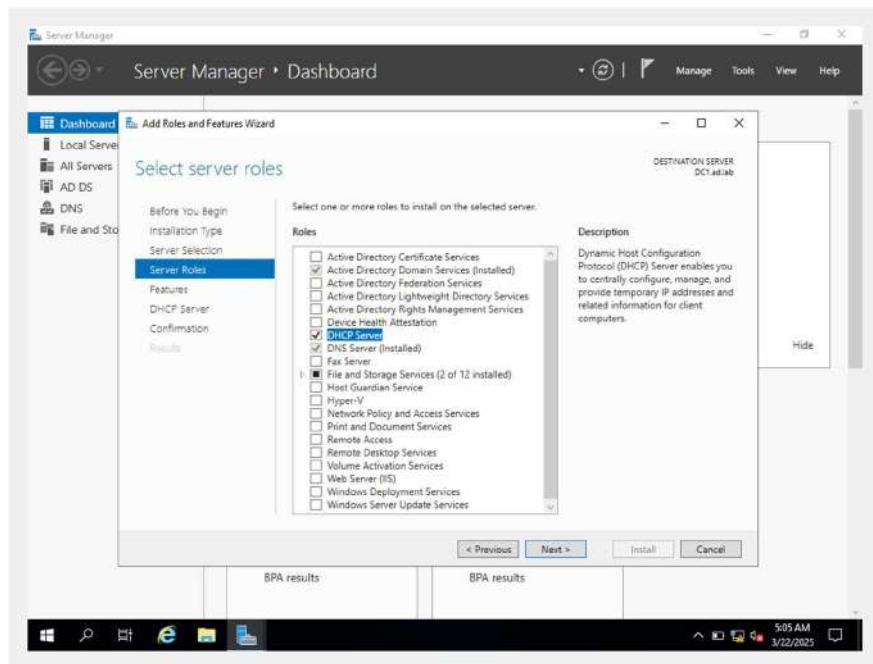
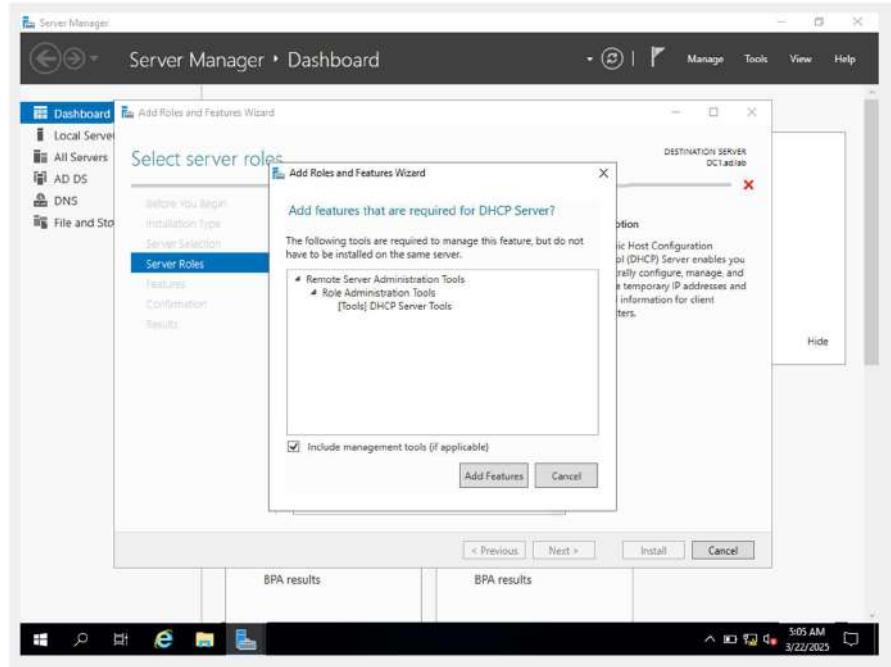
Click on **Next**.



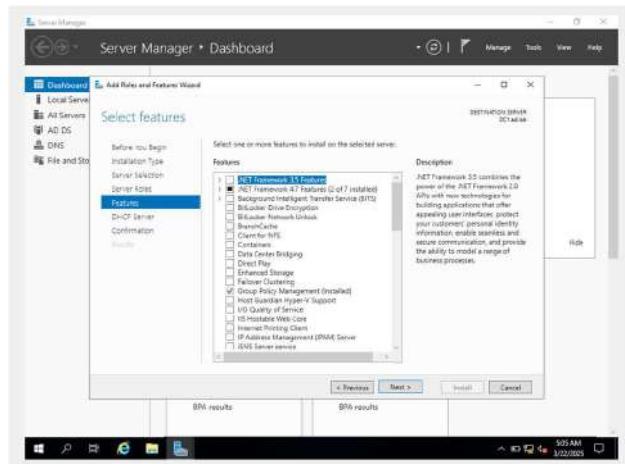
Click on **Next**.



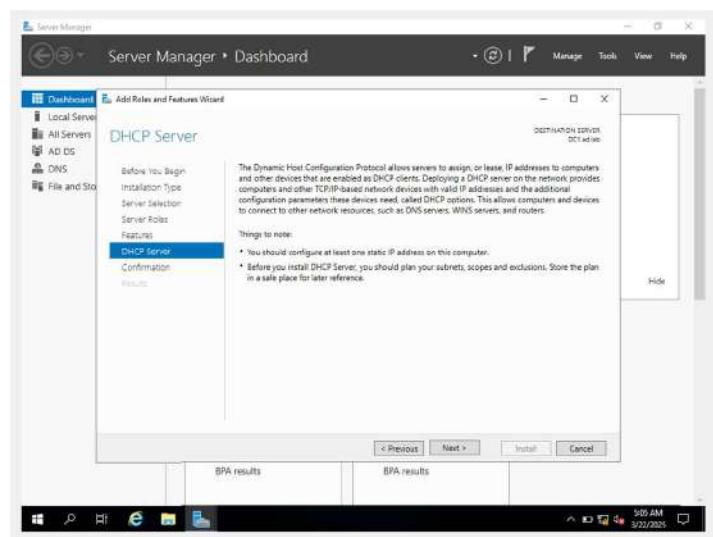
Enable “DHCP Server” then click on “Add Features”.



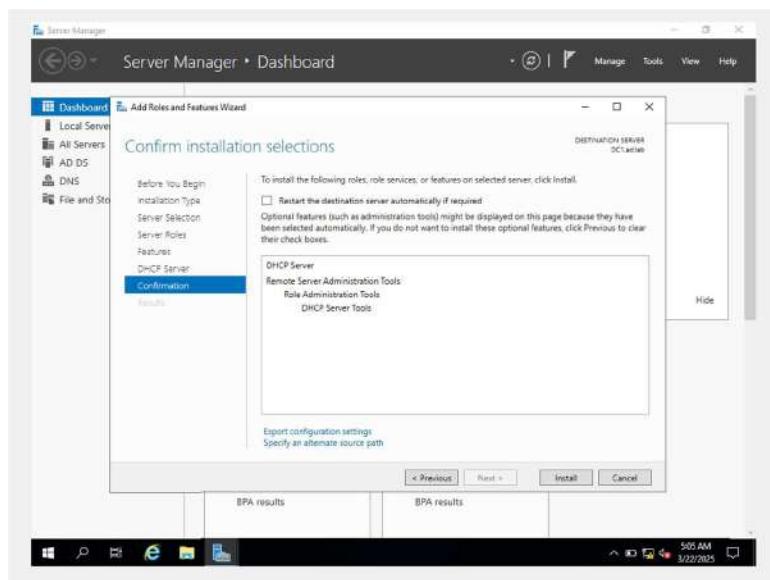
Click on **Next**.



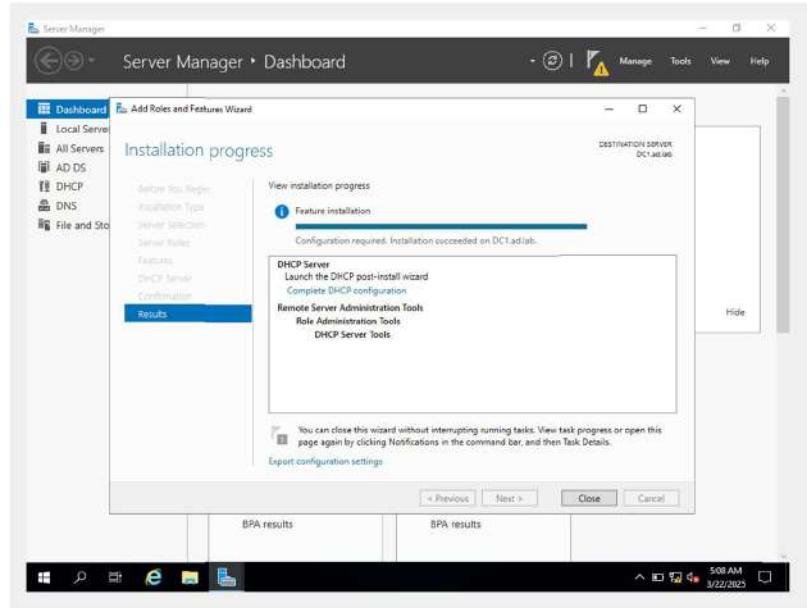
Click on **Next**.



Click **Install** to enable DHCP.

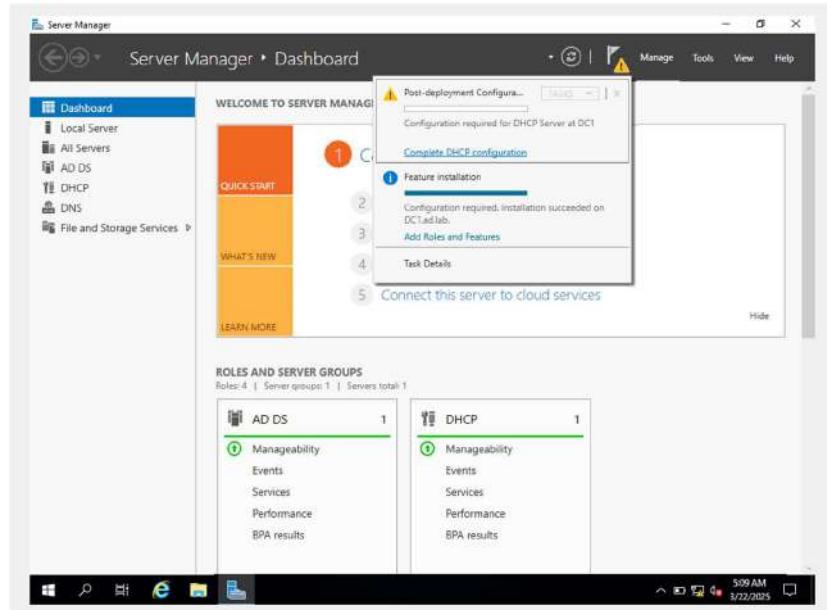


After completion Close it.

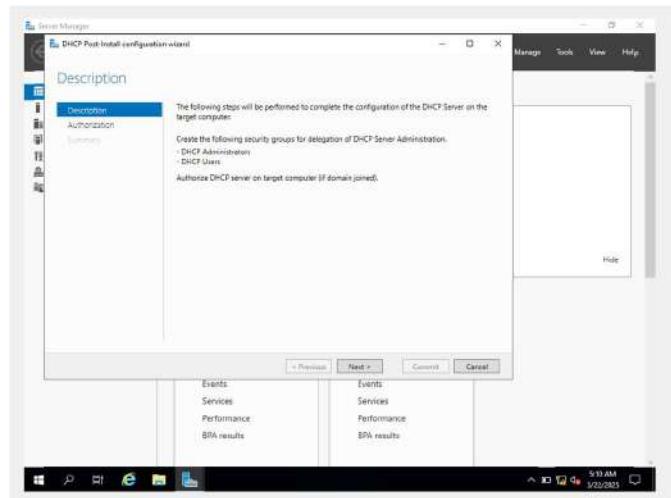


## DHCP Configuration

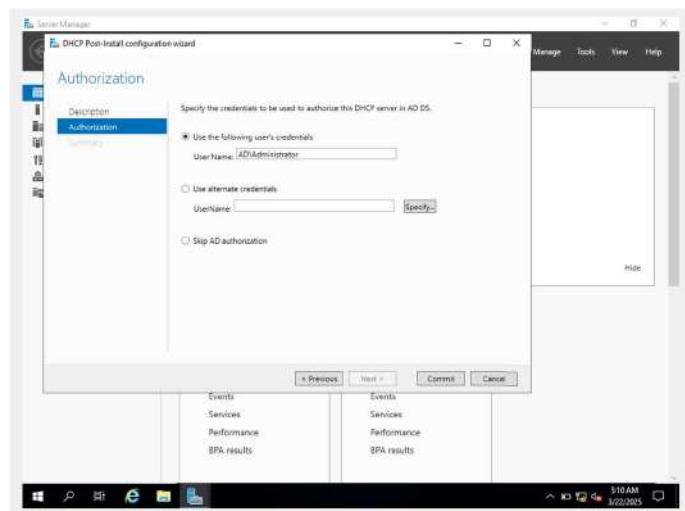
After the installation is complete click on the Flag present in the toolbar of Server Manager and click on “Complete DHCP configuration”.



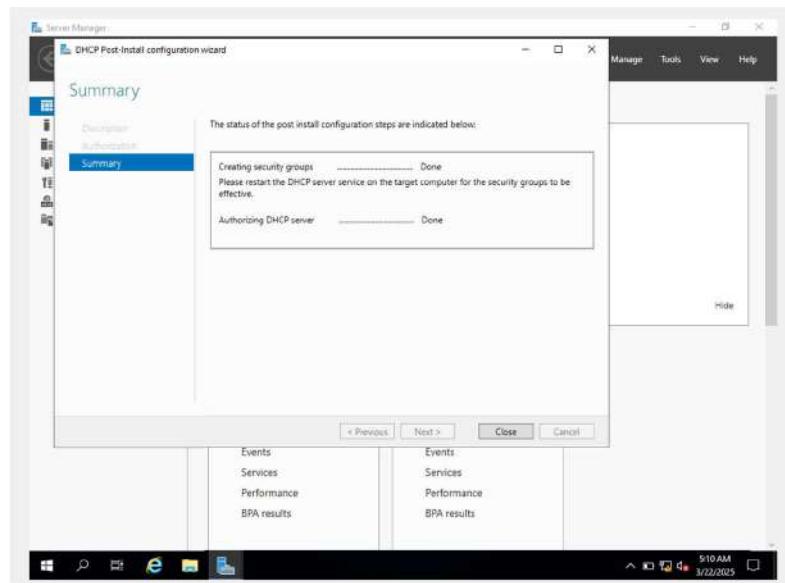
Click on **Next**.



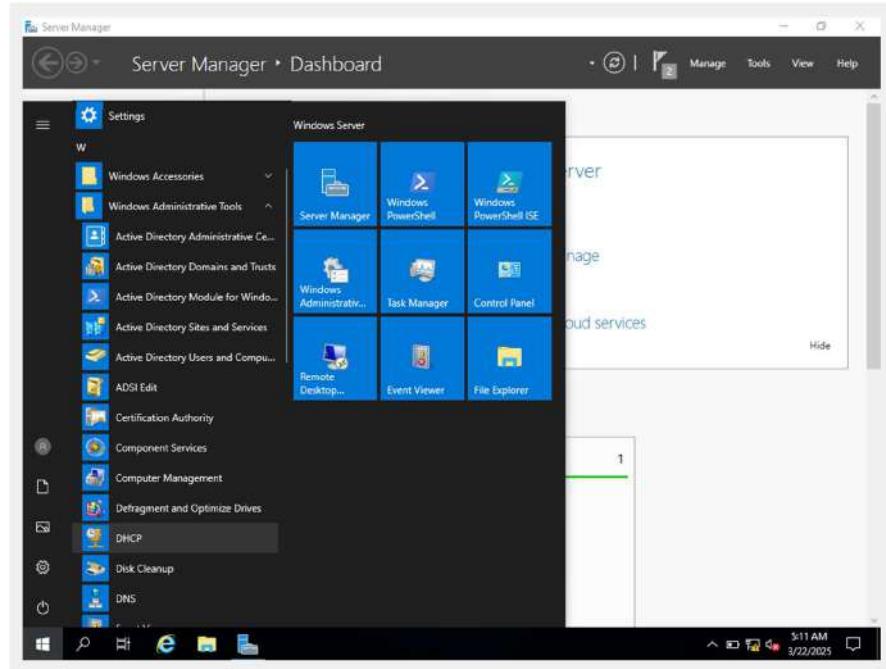
Click on **Commit**.



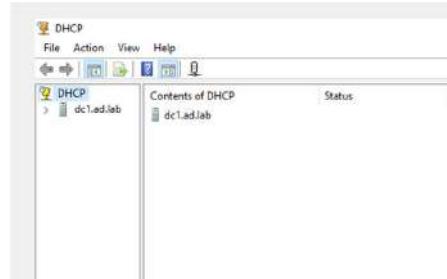
Click on **Close** to complete the installation.



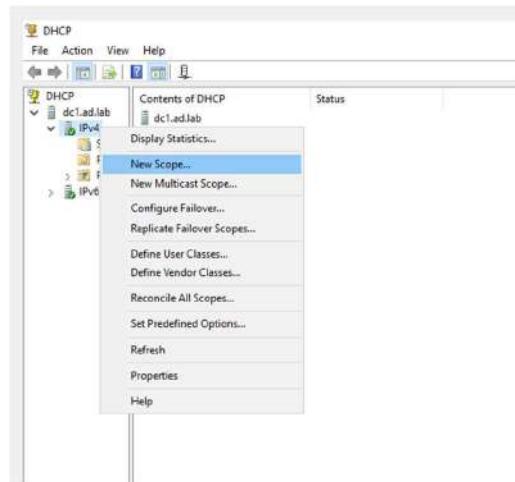
From the Start menu click on “Windows Administrative Tools” and then choose **DHCP**.



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



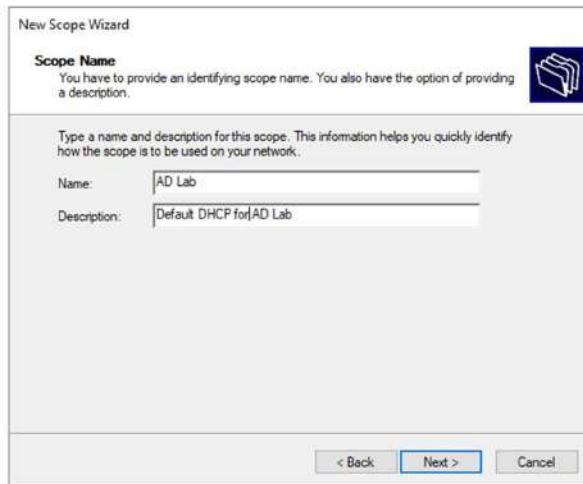
Right-click on **Ipv4**. Then select “New Scope”. The scope defines the range of IP addresses that can be assigned to devices by the DHCP server.



Click Next.



Enter a Name and Description for the new scope.



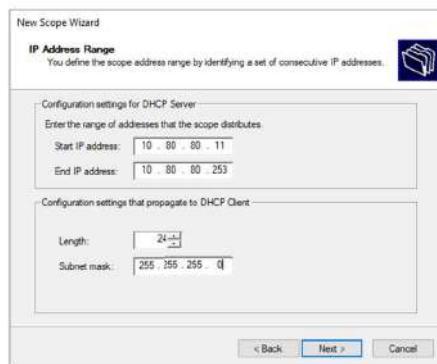
Enter the details as shown below.

Start IP address: **10.80.80.11**

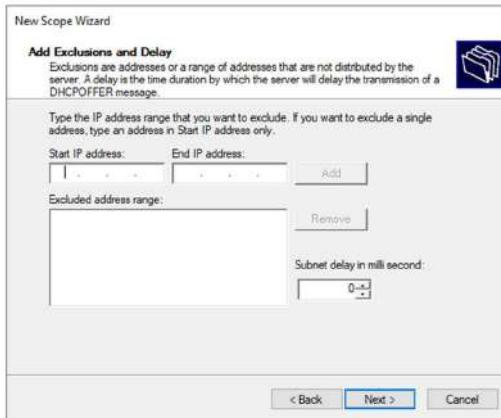
End IP address: **10.80.80.253**

Length: **24**

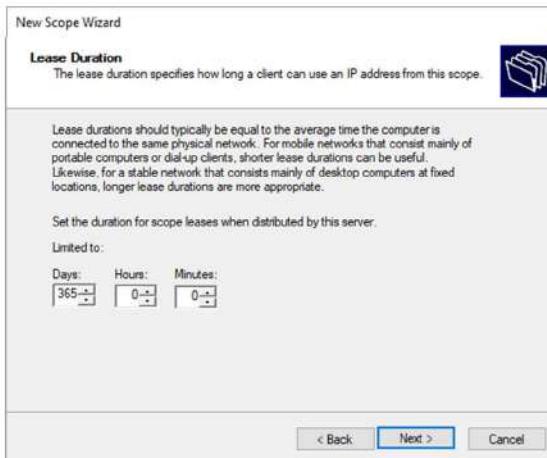
Subnet mask: **255.255.255.0**



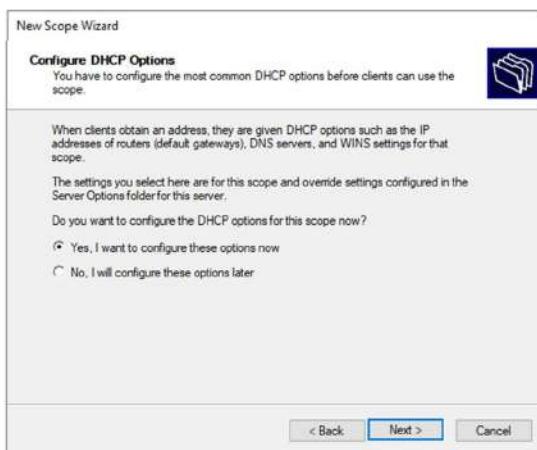
We don't have any Exclusions (static IP assignment). Leave all the options empty and click on **Next**.



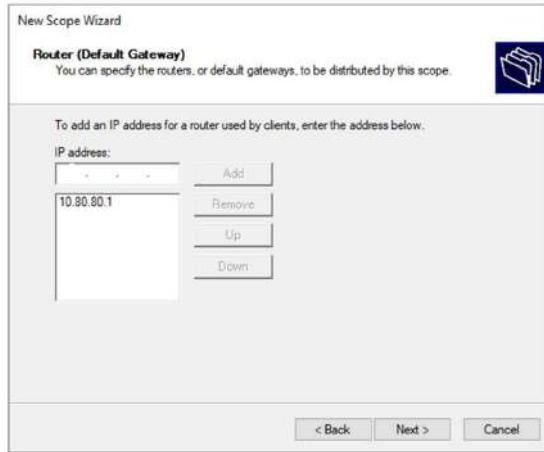
Increase the lease time to **365** days and click on **Next**.



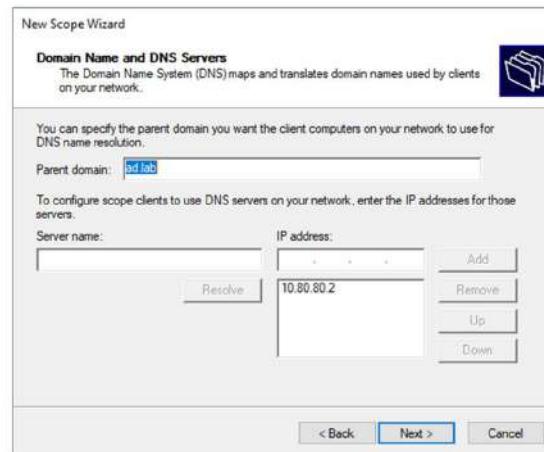
Select "Yes, I want to configure these options now" and click on **Next**.



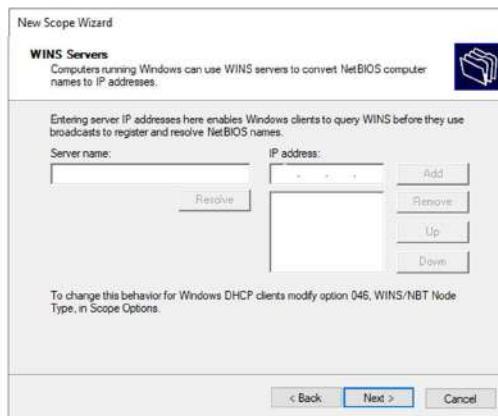
In the IP address field enter the default gateway for the **AD\_LAB** interface (**10.80.80.1**) and then click on **Add**. Once added click on **Next**.



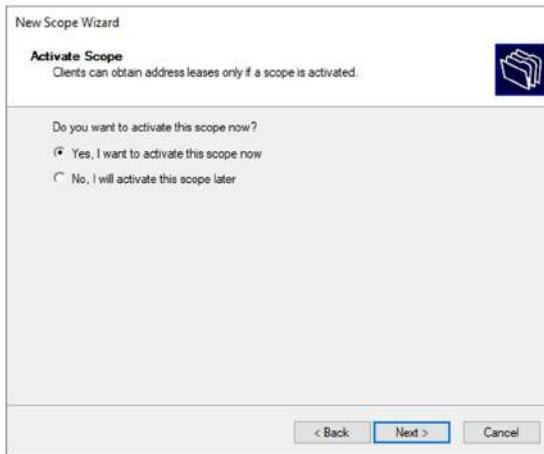
Click on **Next**.



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**.



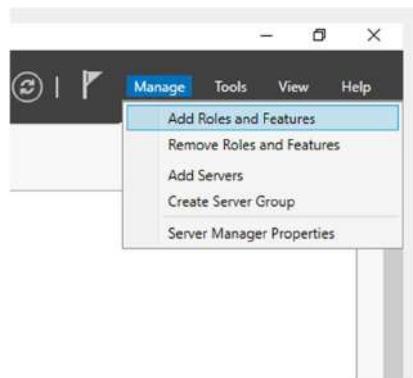
Click on **Finish**.



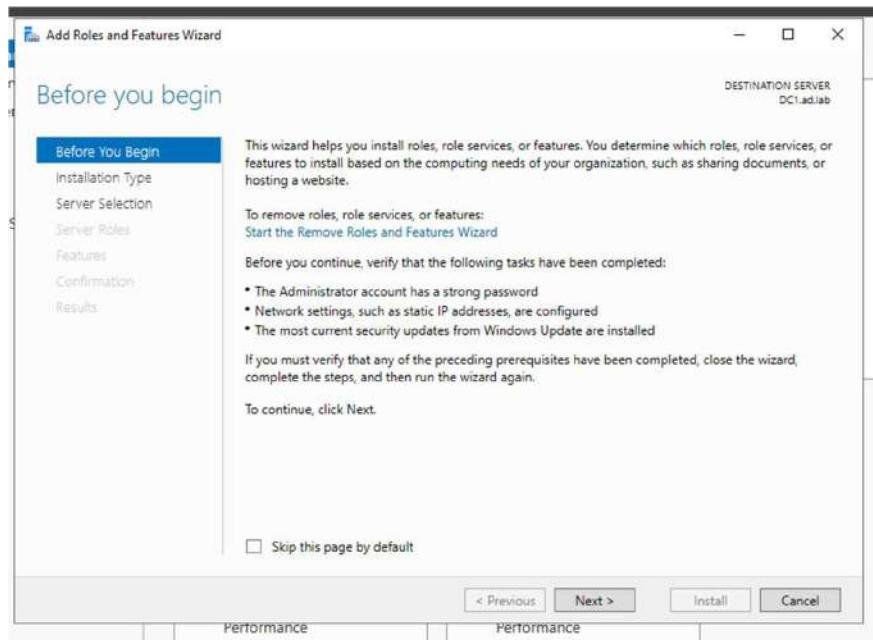
## Domain Configuration

### Certificate Service Installation

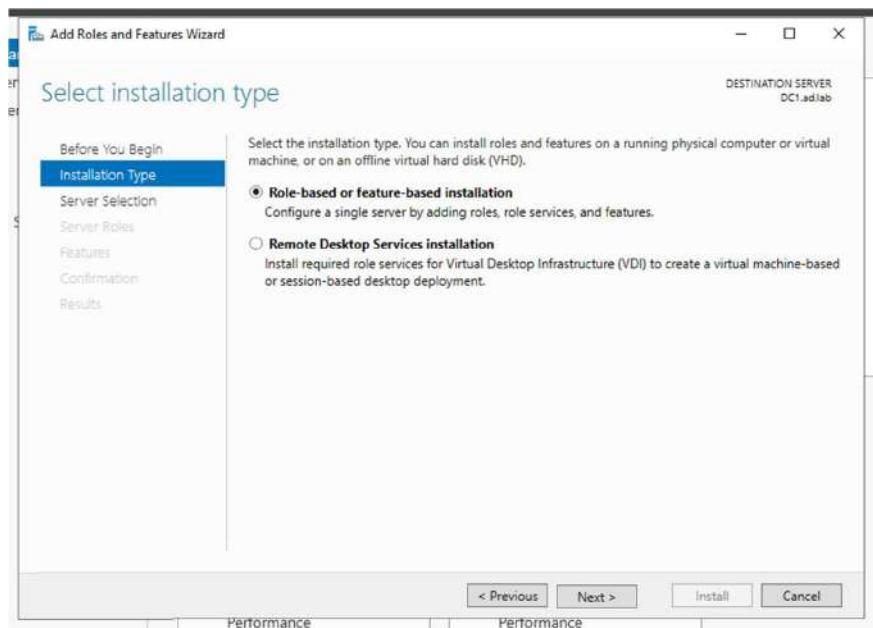
Select **Manage** from the top right corner of Server Manager and then select “Add Roles and Features”.



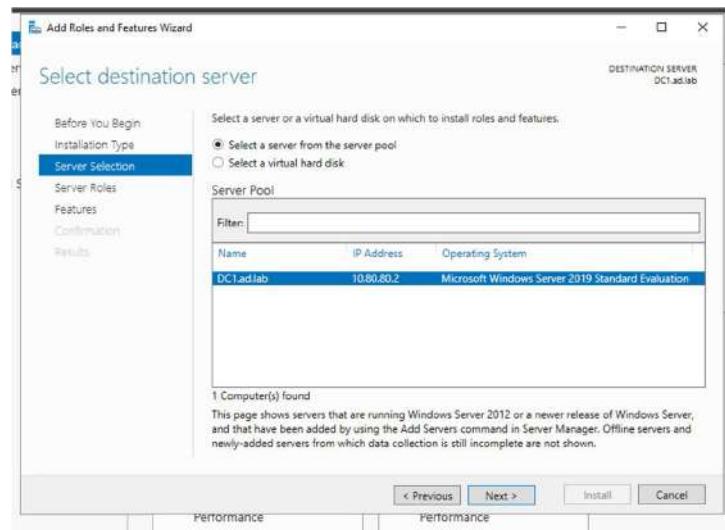
Click Next.



Click Next.

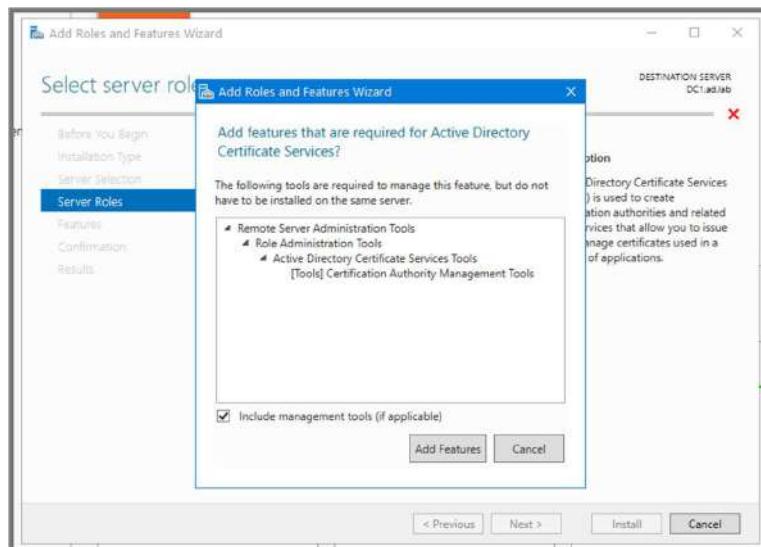


Click Next.

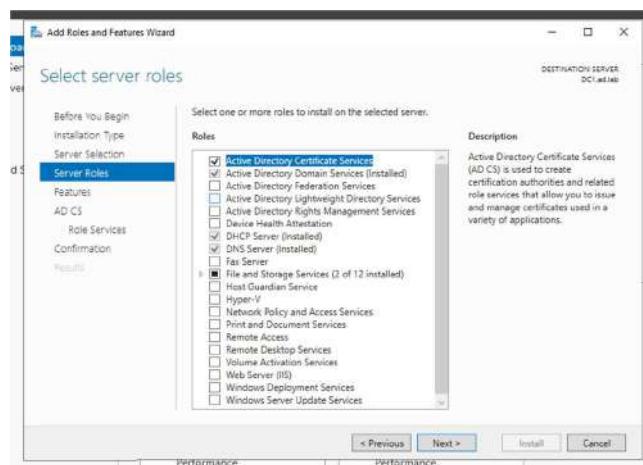


Enable “Active Directory Certificate Services”.

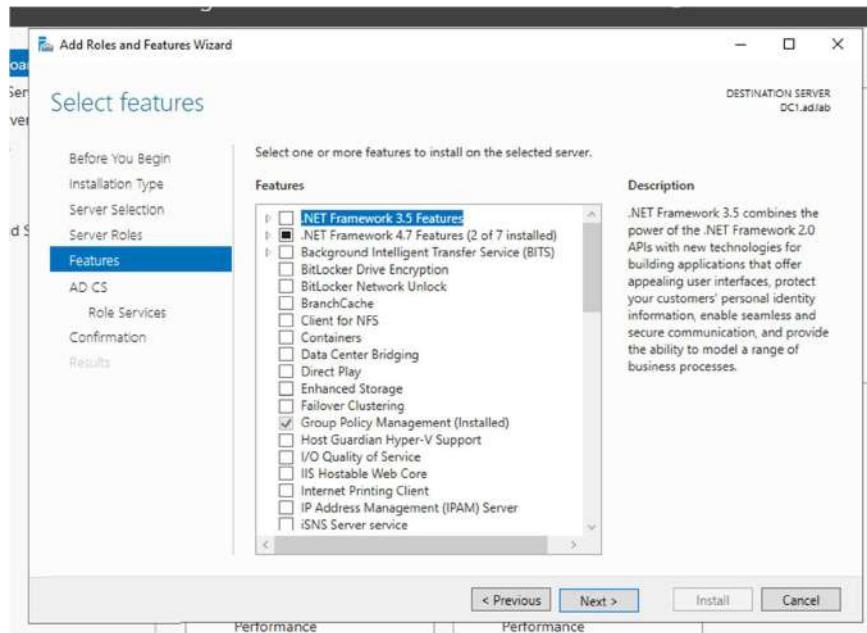
Click on **Add Features**.



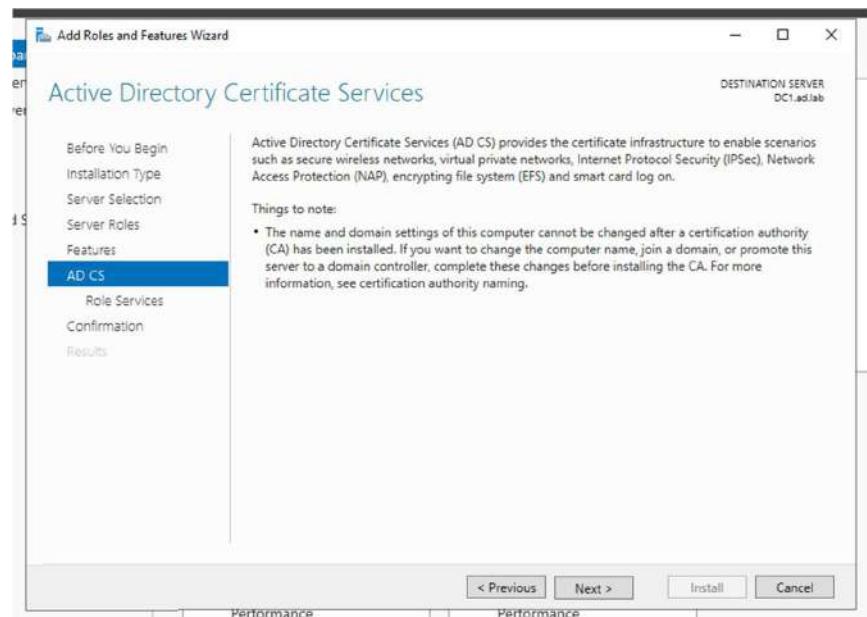
Click **Next**.



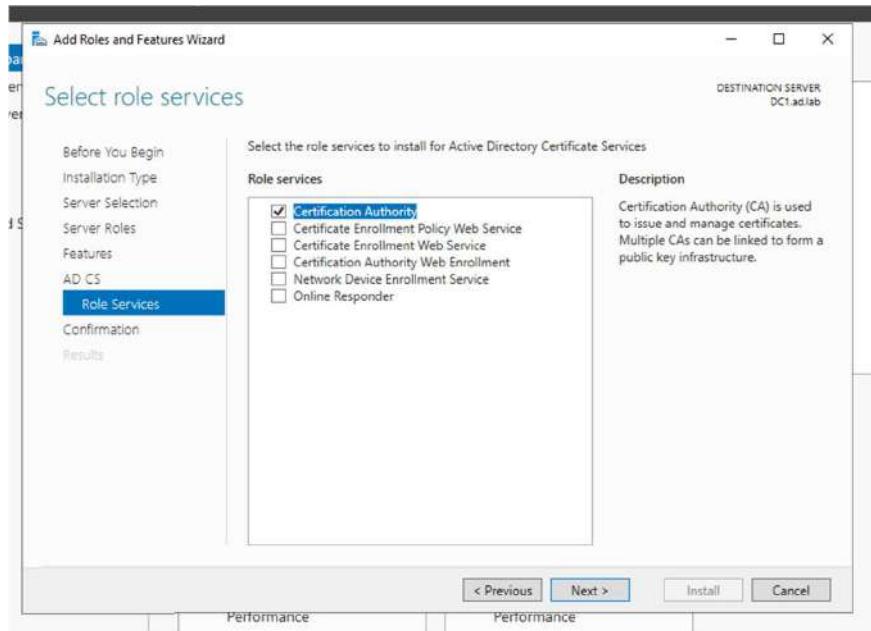
Click **Next**.



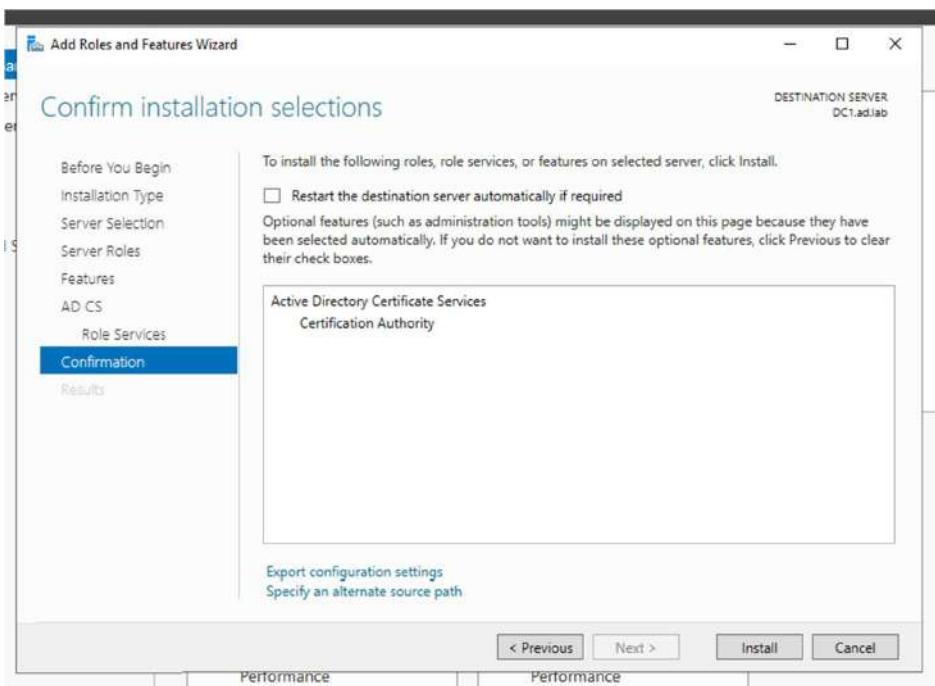
Click **Next**.



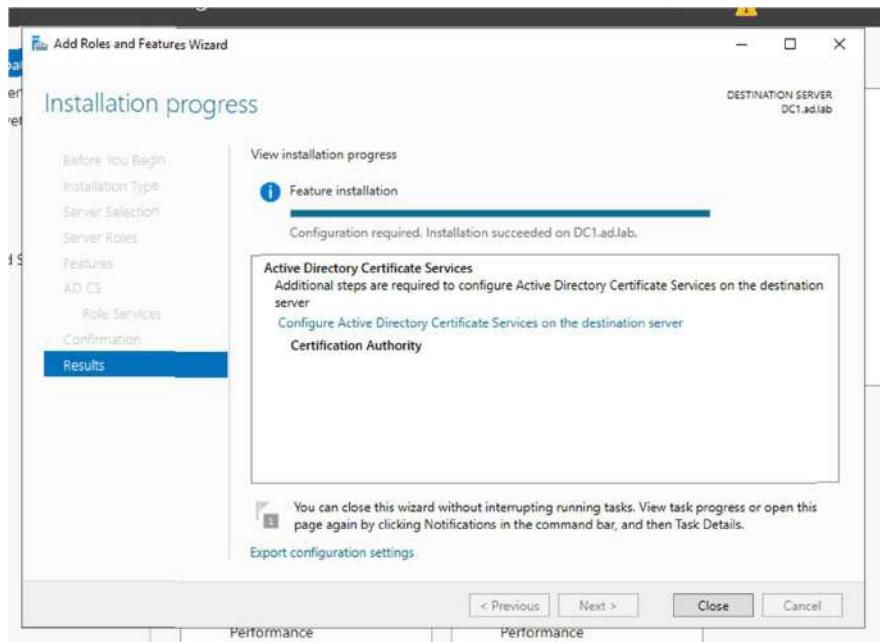
Enable “Certificate Authority”. Click on **Next** to continue.



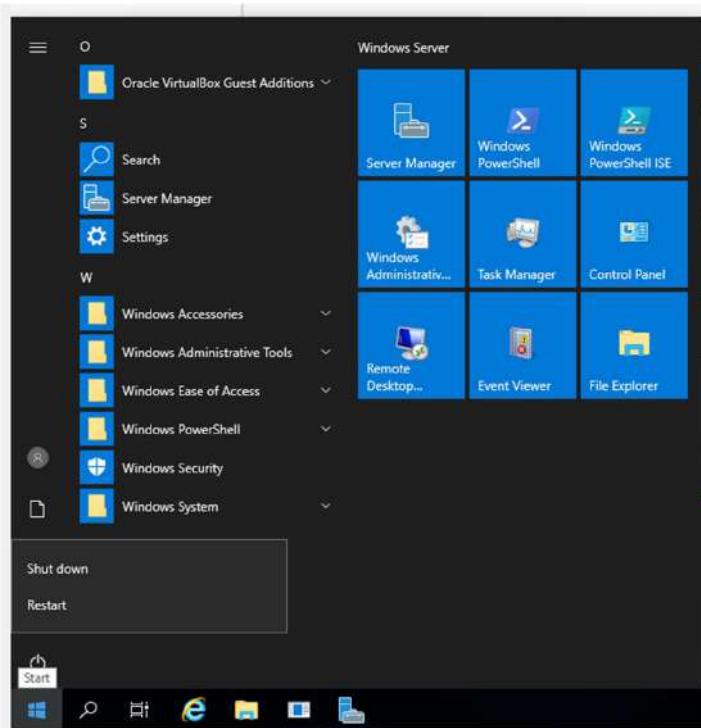
Click on **Install** to start the setup.



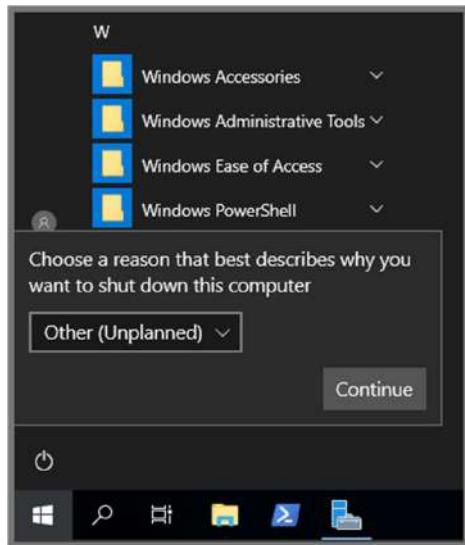
Click on **close** after installation.



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

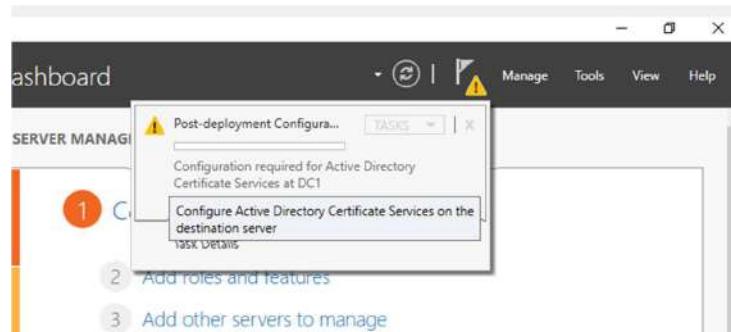


Click on **Continue** to restart the system.

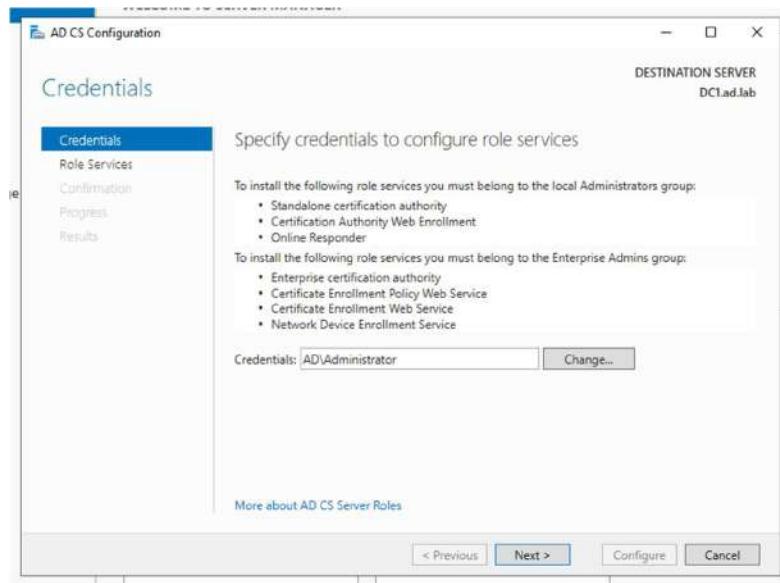


## Certificate Service Configuration

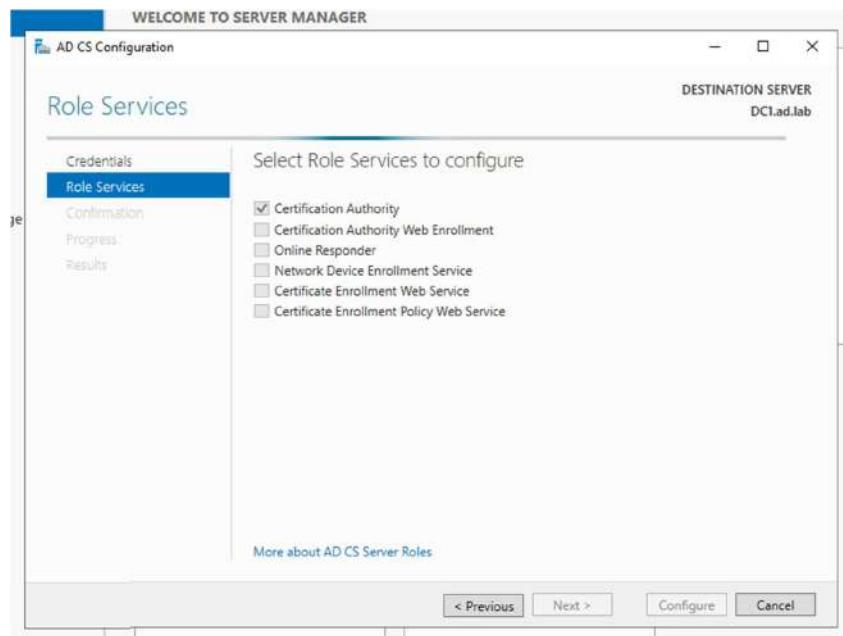
After the restart once Server Manager loads. Click on the Flag icon on the top right side and select “Configure Active Directory Certificate Services”



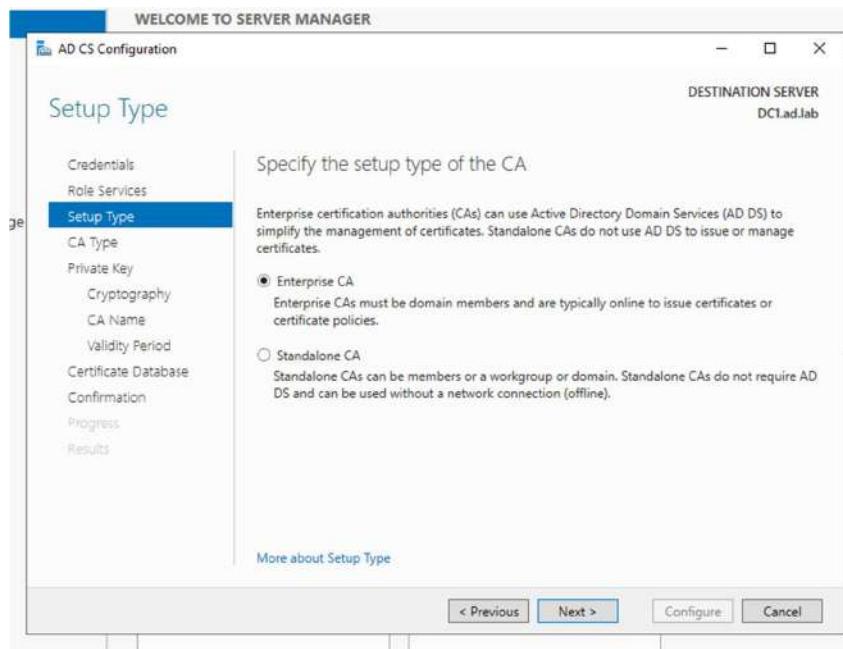
Click on **Next**.



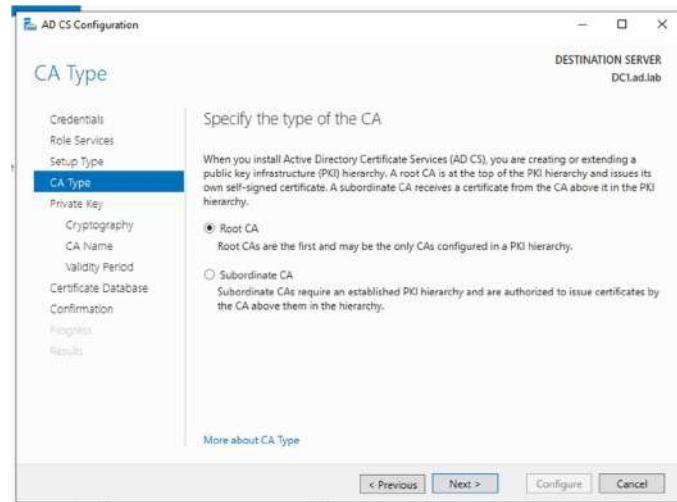
Enable “Certification Authority” and click on **Next**.



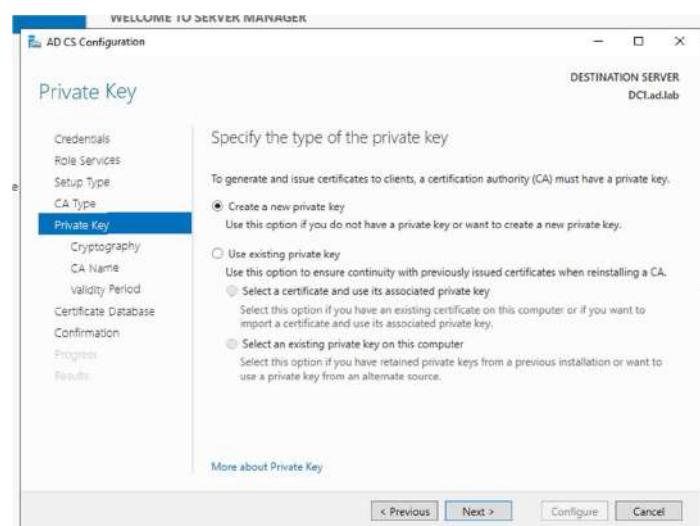
Click on **Next**.



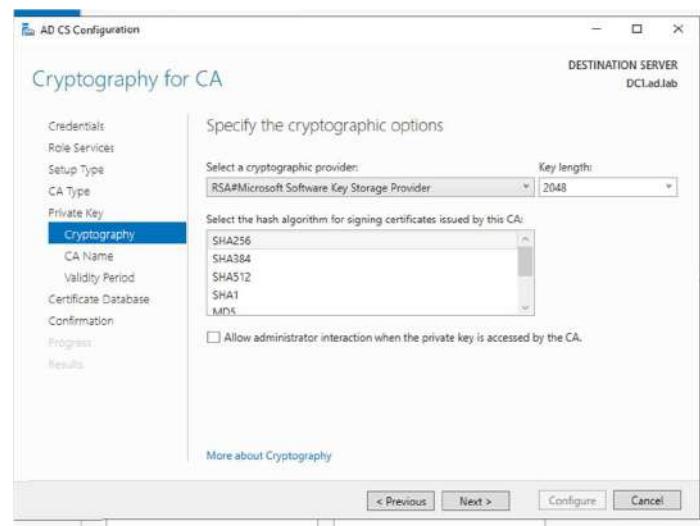
Click on **Next**.



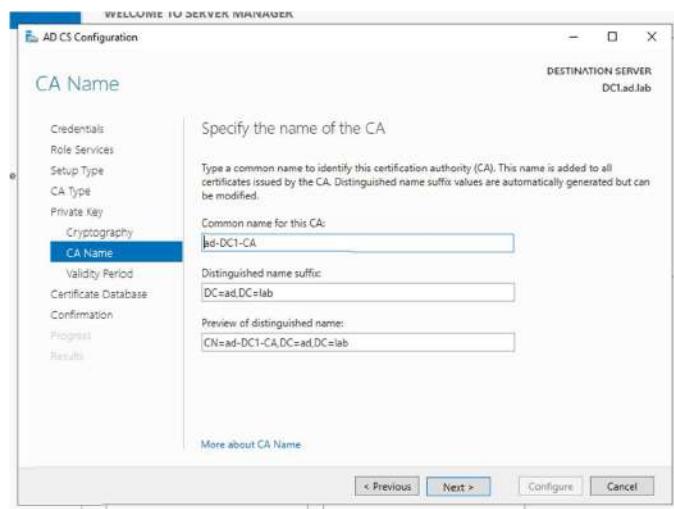
Click on Next.



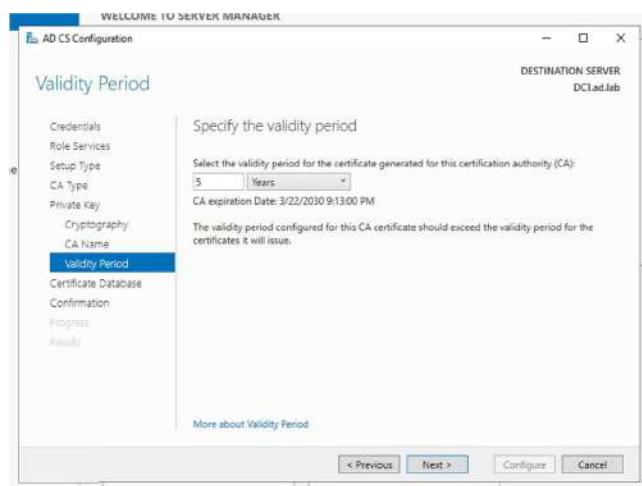
Click on Next.



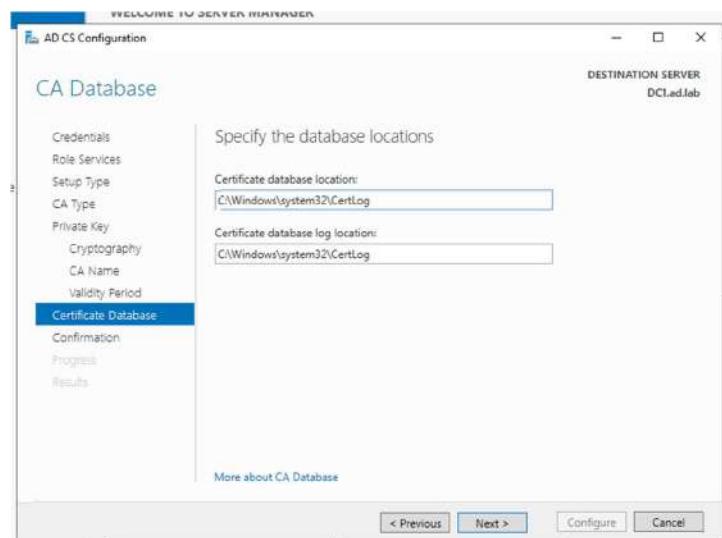
Click on Next.



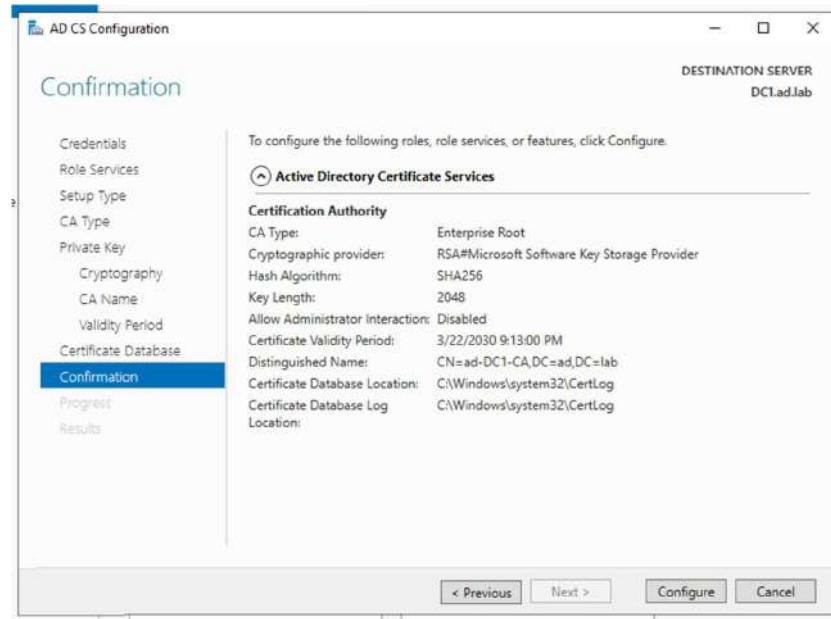
Click on Next.



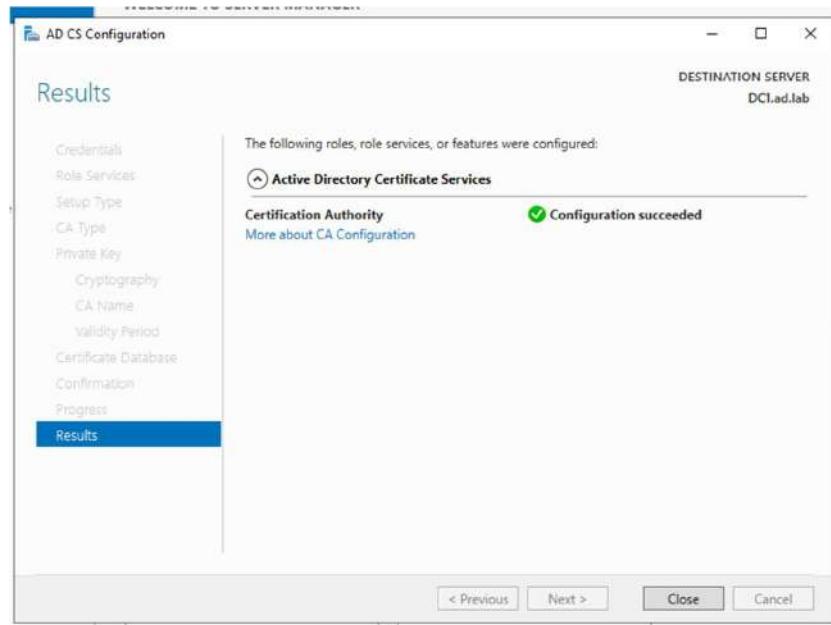
Click on Next.



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



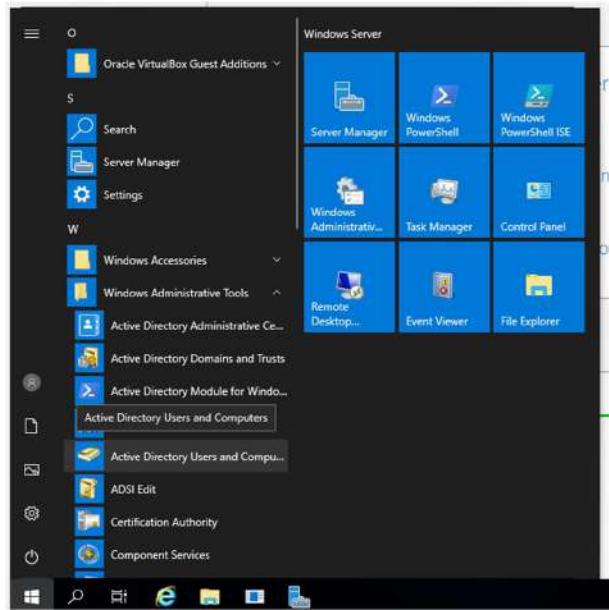
Click on **Close**.



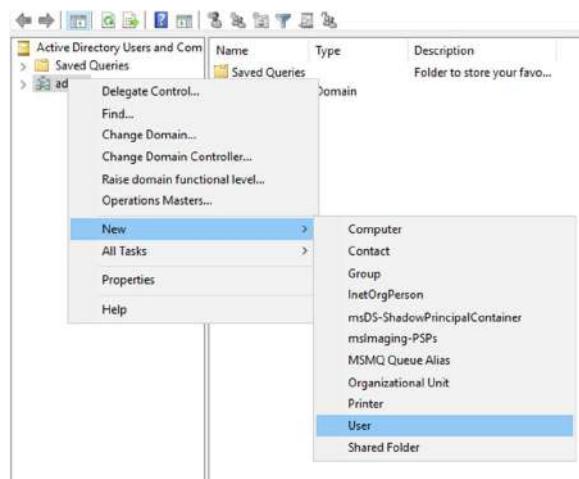
## User Configuration

### AD Admin Setup

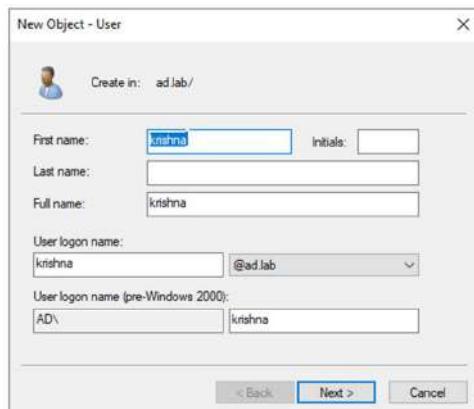
Open the Start menu click on “Windows Administrative Tools” and then select **Active Directory Users and Computers**.



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



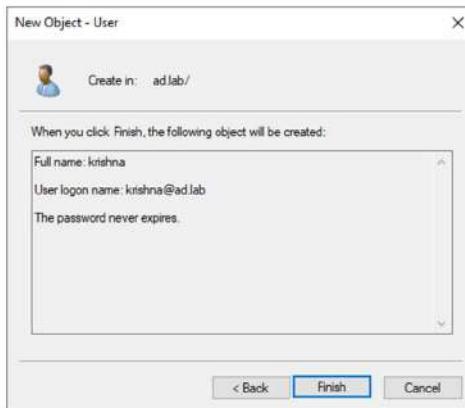
Enter the First Name, Last Name and User logon name for the new user. This user will be the **Administrator** for the Domain Controller.



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



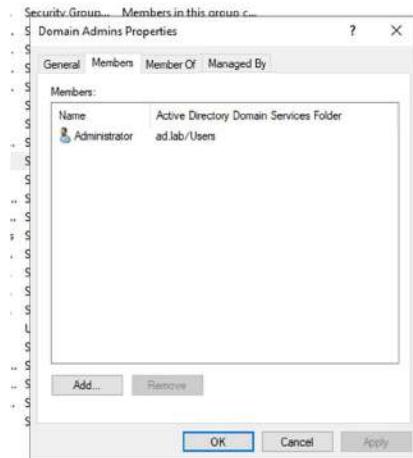
Click on **Finish**.



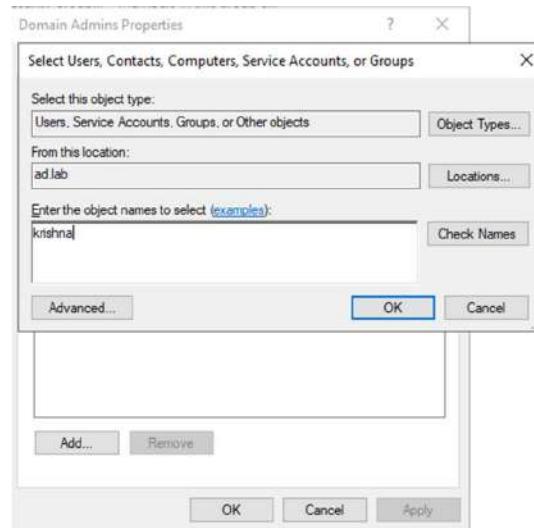
Expand the dropdown on the domain name from the sidebar. Click on **Users**. Then double-click on “Domain Admins”.

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DHCP Admin...	Security Group...	Members who have ad...
DHCP Users	Security Group...	Members who have vie...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group ca...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...

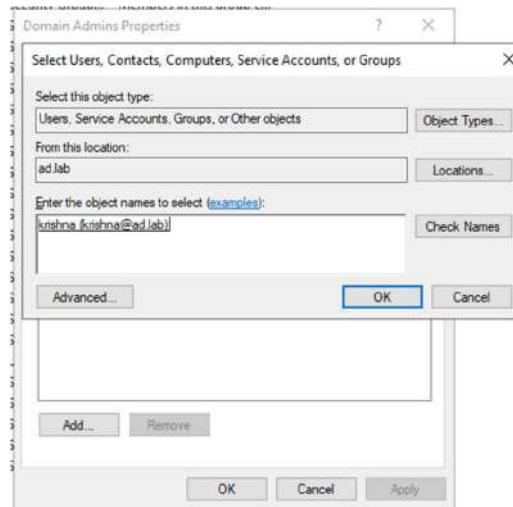
Go to **Members** -> **Add**.



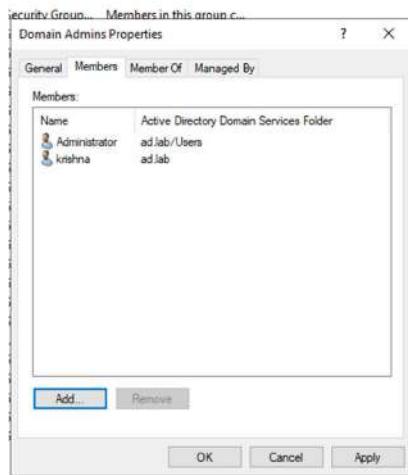
Enter the name of the user and check on **Check Names**.



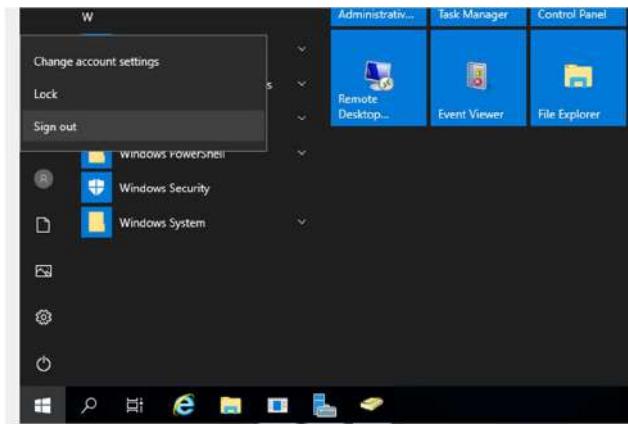
Click on **OK**.



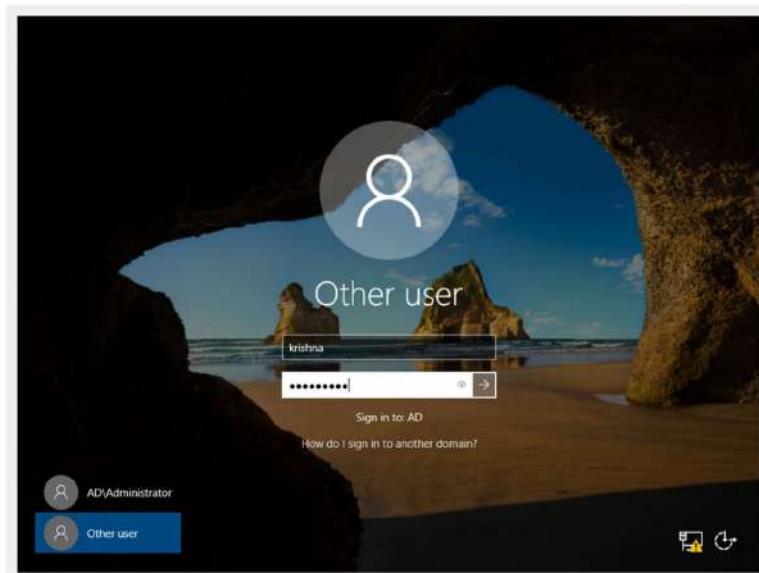
Click on **Apply** then **OK** to persist the changes.



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

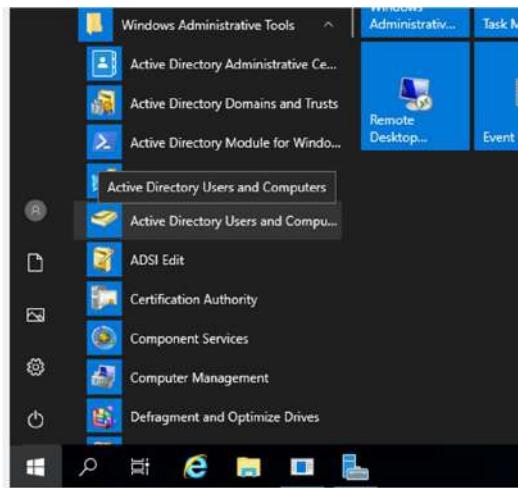


From the login screen select “Other user”. Then enter the login name and password that was configured for your domain administrator.

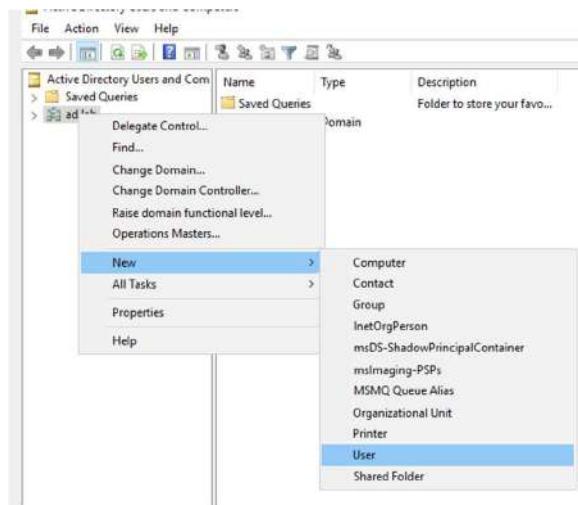


## AD User 1 Setup

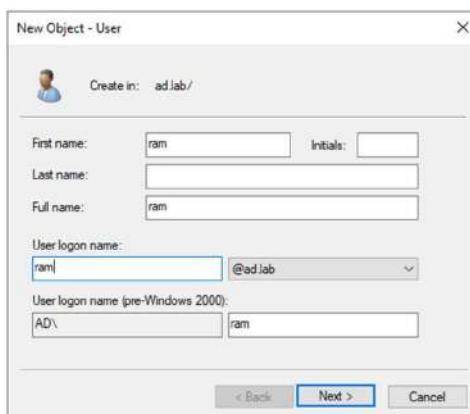
Open the Start menu. Select “Windows Administrative Tools” and then choose **Active Directory Users and Computers**.



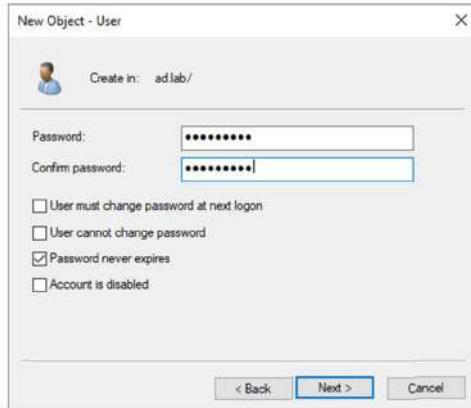
Right-click on the domain name from the sidebar. Select **New -> User**.



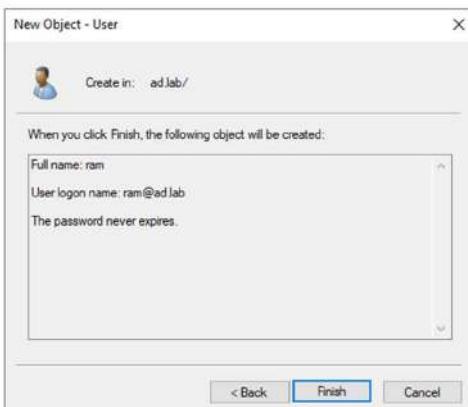
Enter the details for the user.



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

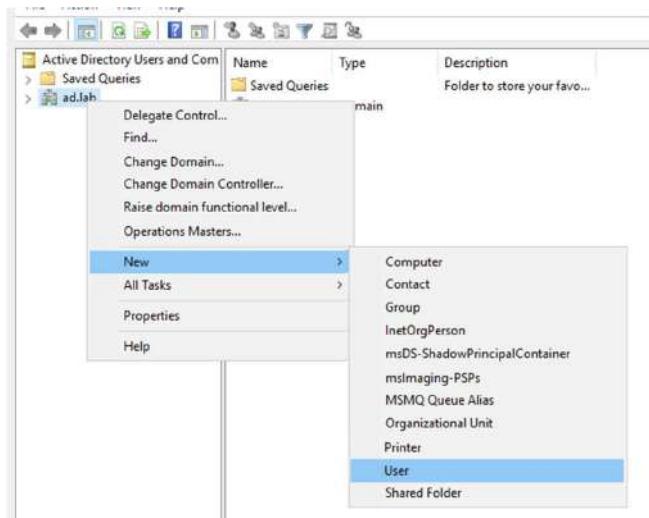


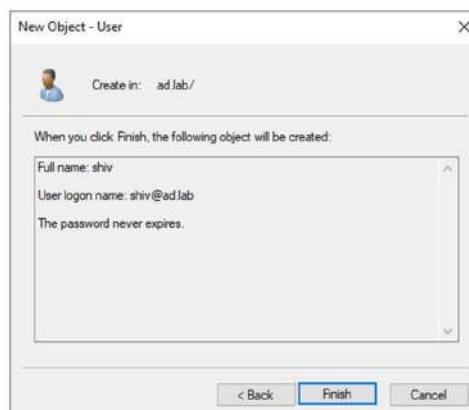
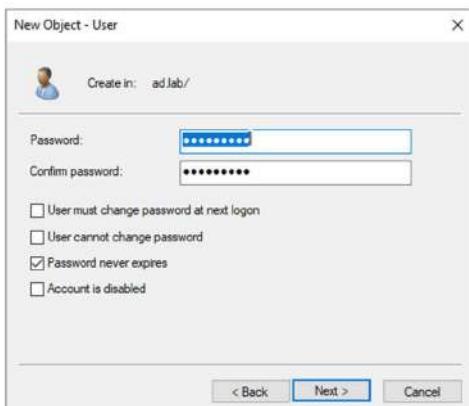
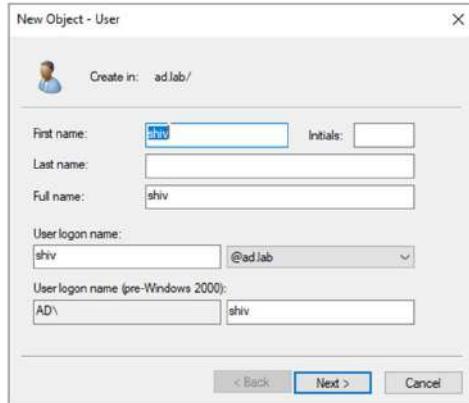
Click on **Finish**.



## AD User 2 Setup

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



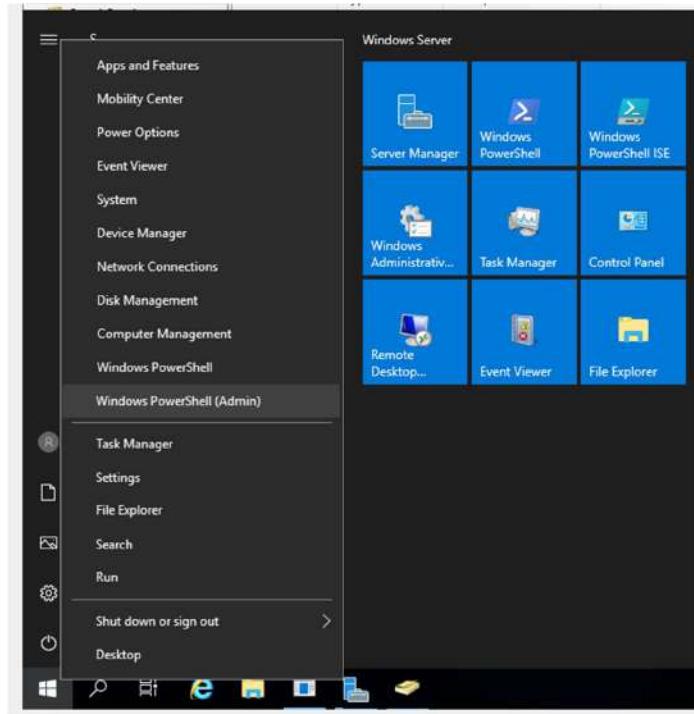


## Making AD Lab Exploitable

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.

```
PS C:\Windows\system32> Set-SmbShare -Name Public -Path C:\ -ShareType FileSystem -FullAccess $true -Force
SmbShareName : Public
SmbPath      : C:\
SmbFullAccess: True
SmbInheritance: InheritAll
SmbSDDL      : O:FA((everyone,(X,WD,GA,))n)
ShadowCopy   : False
ShareState   : Online
ShareType    : FileSystemDirectory
SmbInstanceId: Default
Special      : False
Temporary    : False
Volume       : \\?\Volume{e7c87acf-0000-0000-0000-002200000000}\Public
PSCoputerName:
PresetPathAcl: System.Security.AccessControl.DirectorySecurity

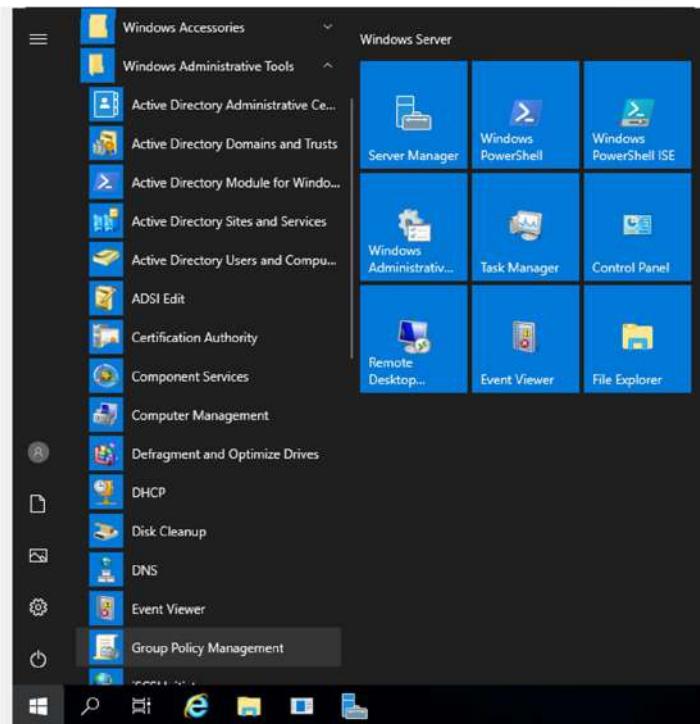
NullSessionShares : {C:\Common}
PSPath           : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
PSParentPath     : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer
PSChildName     : Parameters
PSDrive          : HKLM
PSProvider       : Microsoft.PowerShell.Core\Registry

    [+] Created Public SMB Share
Ok.

    [+] Firewall Turned Off
Restarting in 30 seconds...
```

## Group Policy Configuration

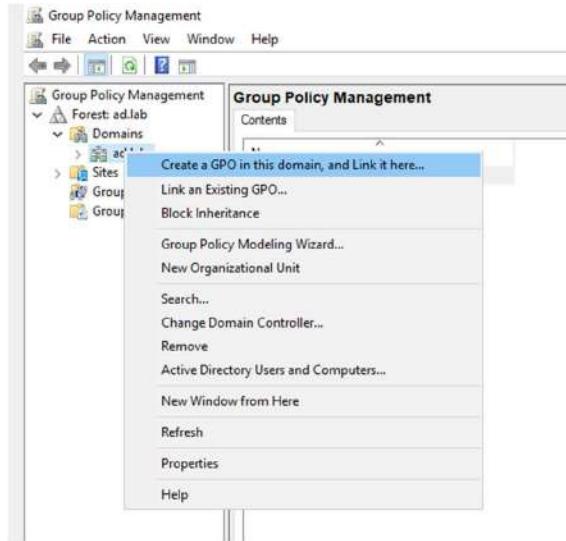
After the system restarts open the Start menu and click on “Windows Administrative Tools” then choose **Group Policy Management**.



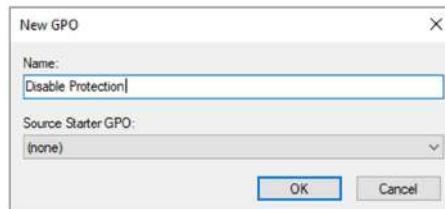
Expand “Forest” and then expand “Domains”.

## Disable Windows Defender and Firewall

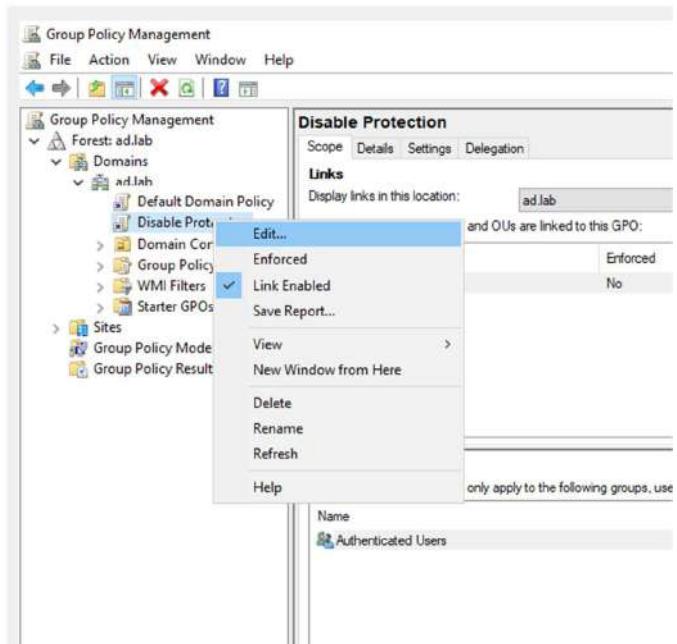
Right-click on the domain name. Select “Create a GPO in the domain and link here”.



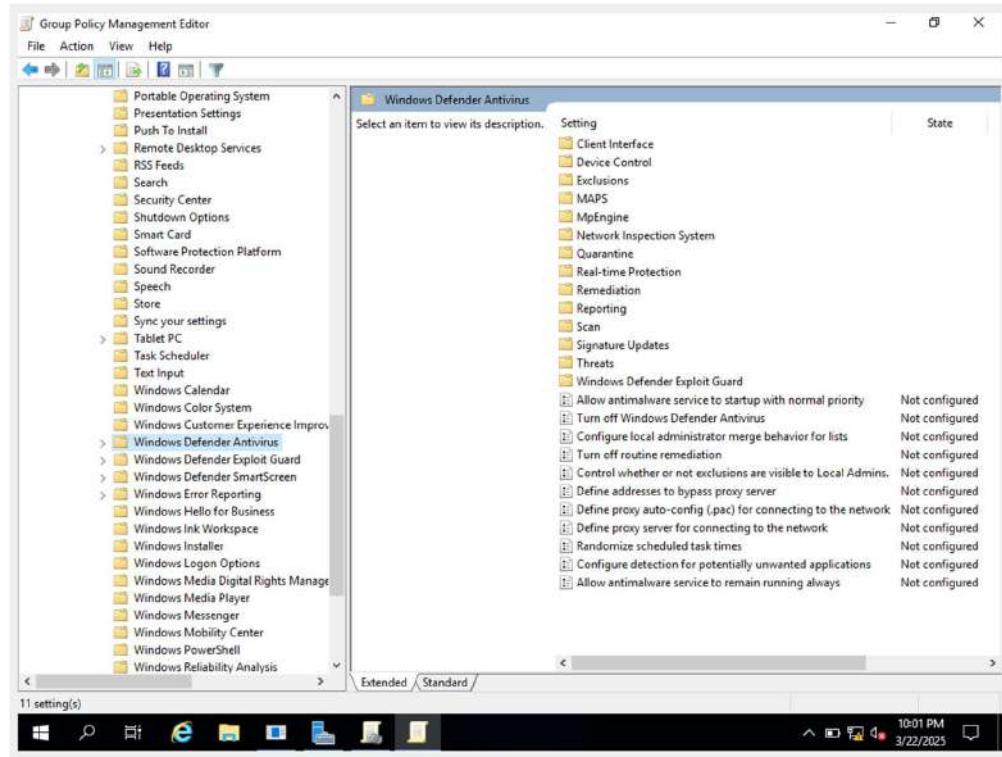
Give the GPO the name **Disable Protections**.



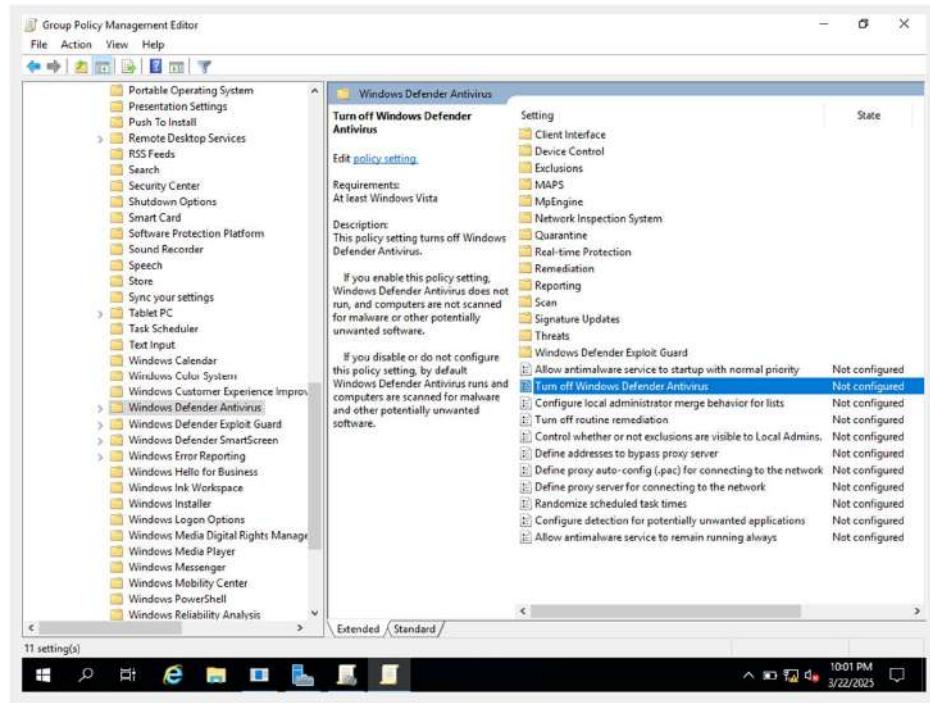
Expand the domain name. Right-click on “Disable Protections” and choose **Edit**.



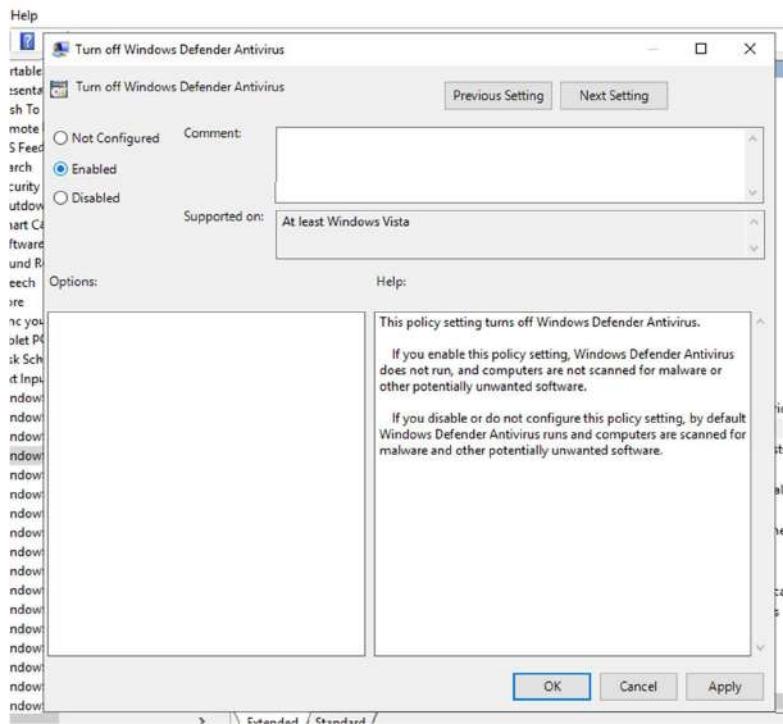
This will open the **Group Policy Management Editor**. From the sidebar go to the following folder: **Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Defender Antivirus**.



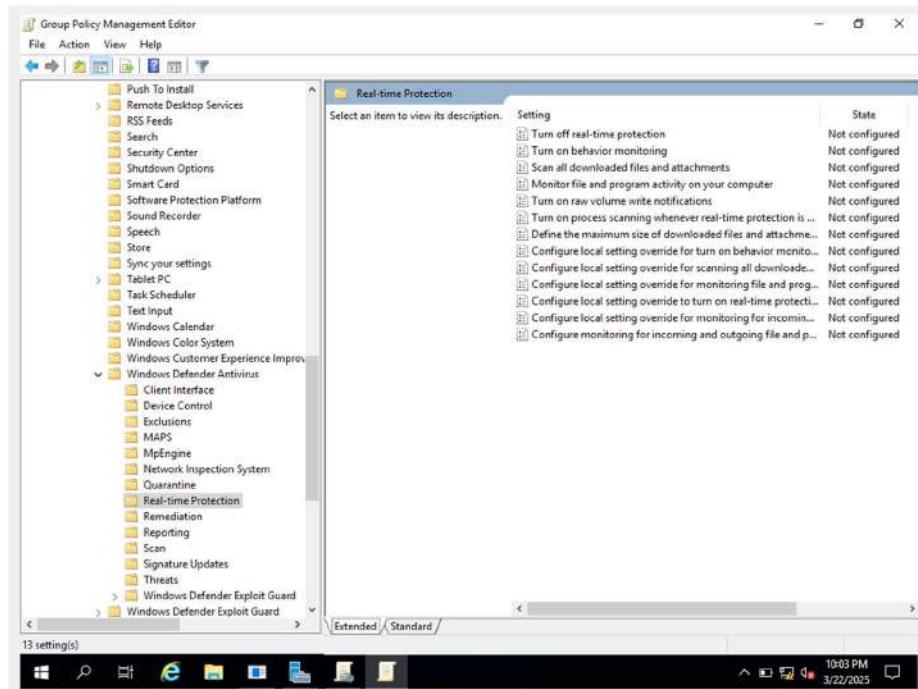
Select “Windows Defender Antivirus”. From the right side select “Turn off Windows Defender Antivirus” and click on **Edit policy setting**.



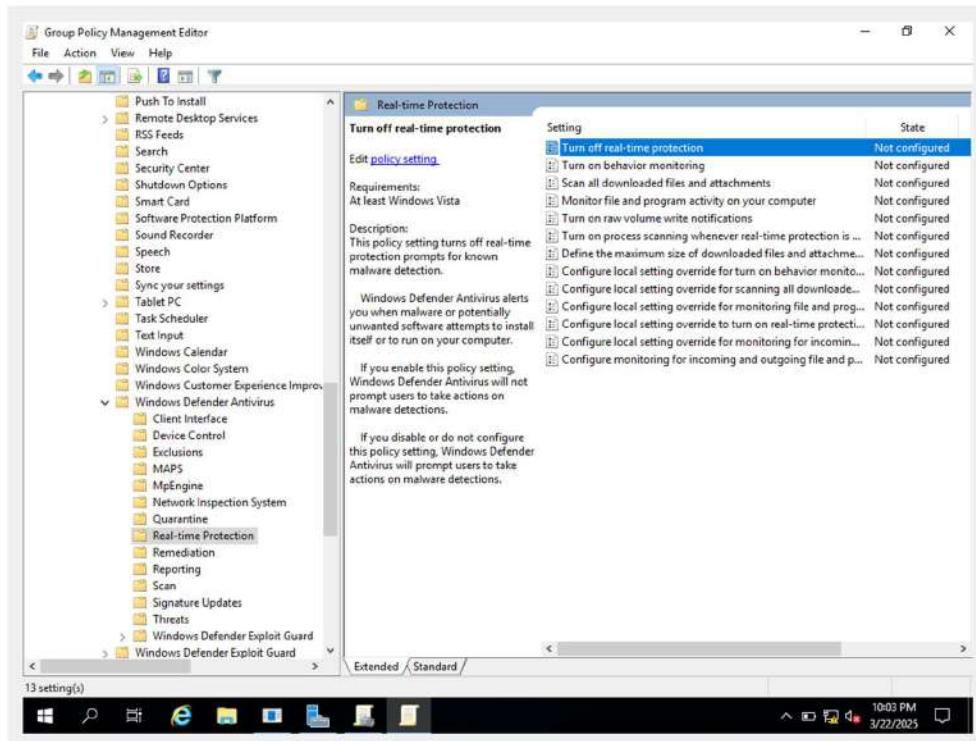
Set it to **Enabled**. Click on **Apply** then **OK** to save the changes.



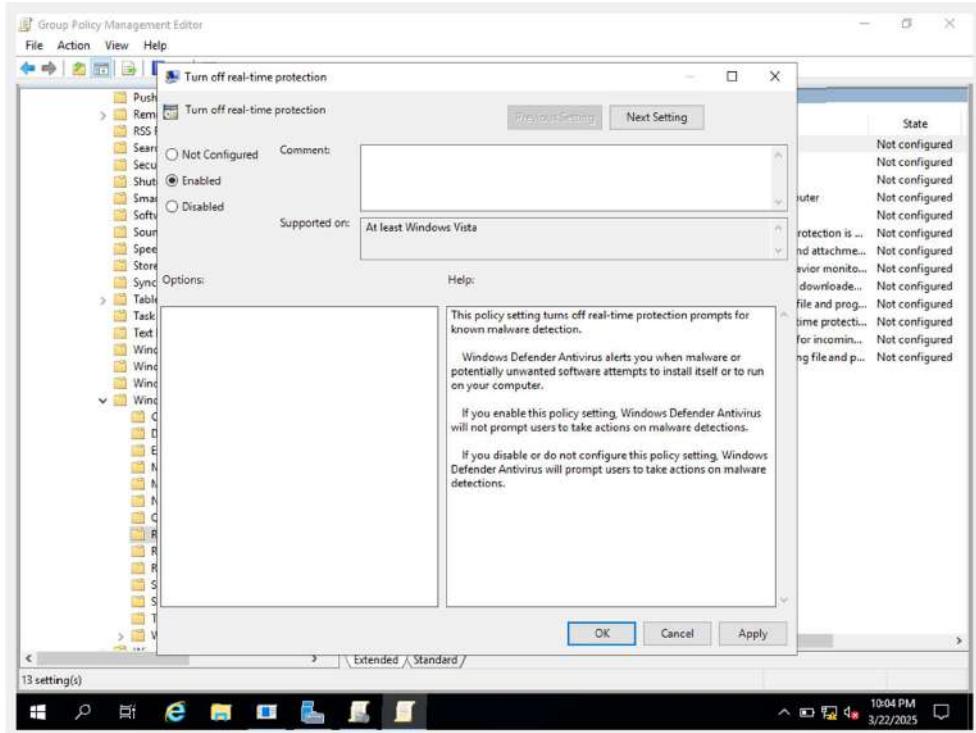
Double-click on **Real-time Protection**



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

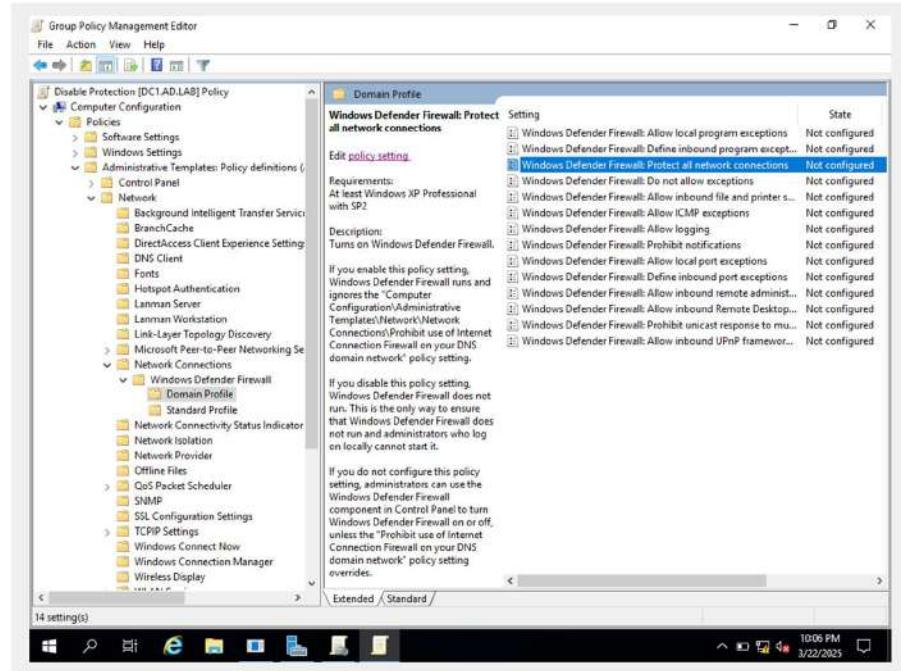


Set it to **Enabled**. Click on **Apply** then **OK** to save the changes.

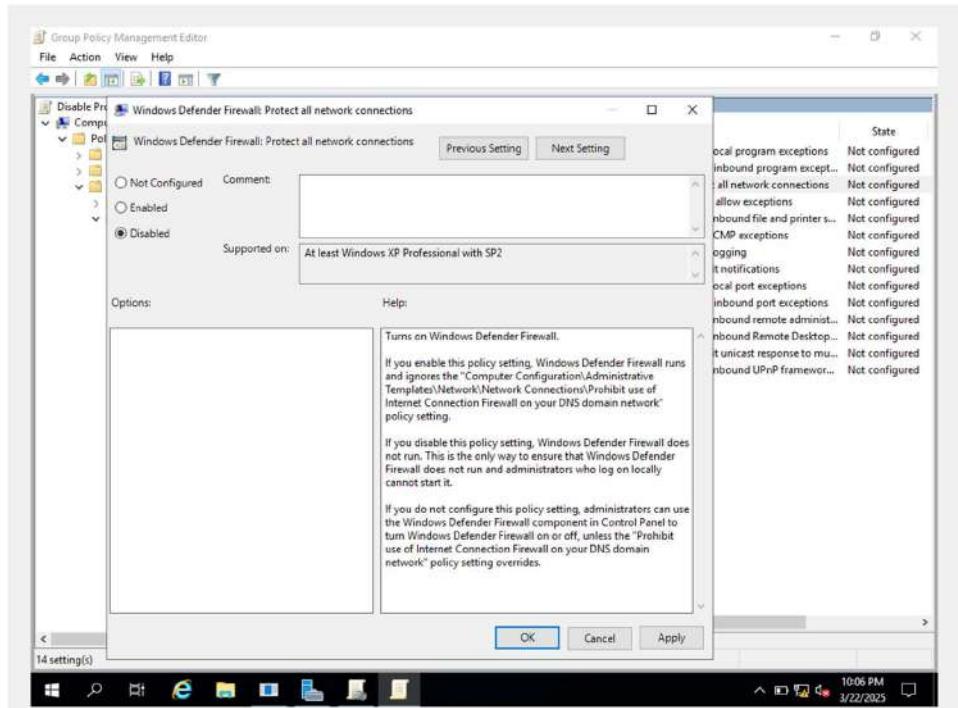


Expand the sidebar folders to the following: **Computer Configuration -> Policies -> Administrative Templates -> Network -> Network Connections -> Windows Defender Firewall -> Domain Profile.**

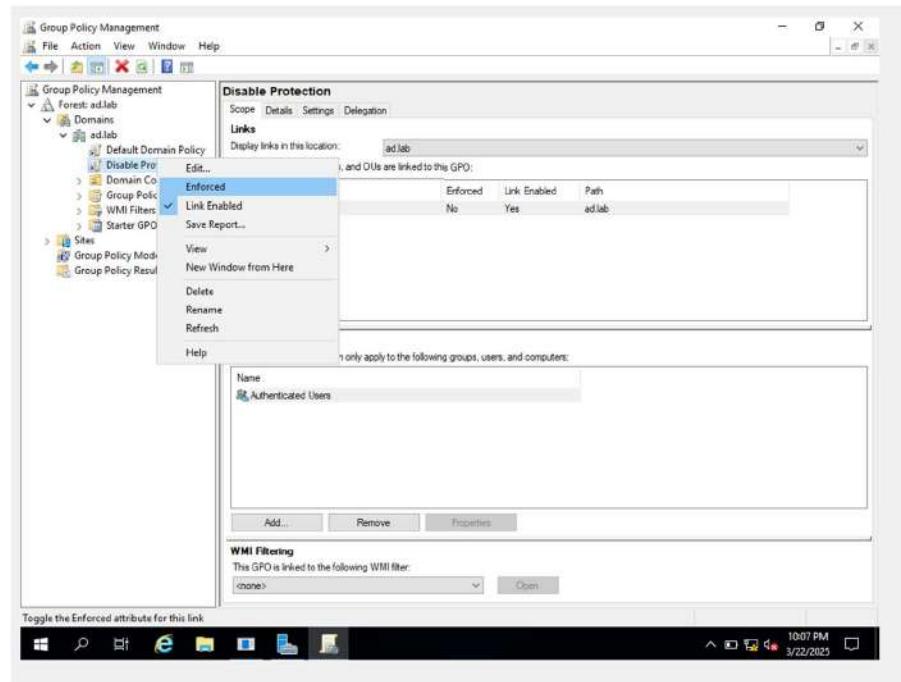
Select “Windows Defender Firewall: Protect all network connections”. Click on “Edit policy settings”.



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

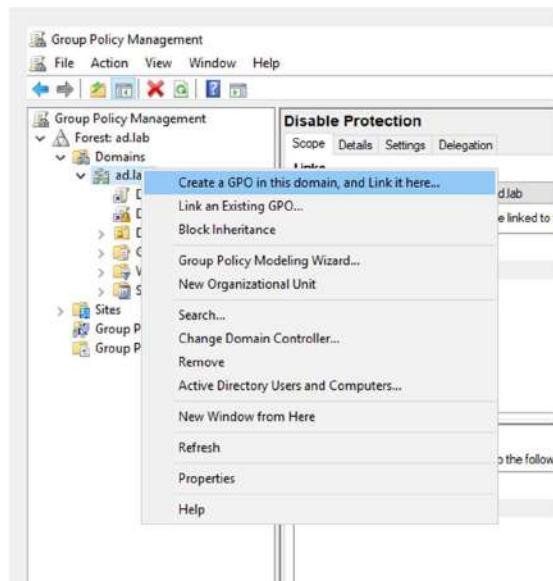


Close Group Policy Management Editor. From the sidebar of Group Policy Management right-click on “Disable Protections” and choose “Enforced”.

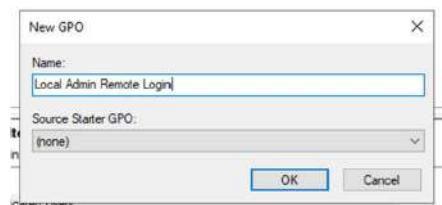


## Enable Remote Login for Local Admins

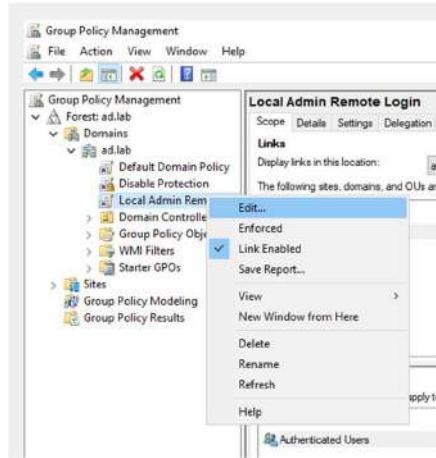
Right-click on the domain name. Select “Create a GPO in the domain and link here”.



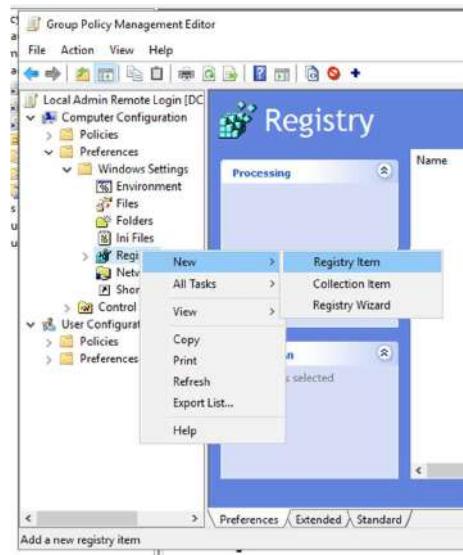
Give the GPO the name **Local Admin Remote Login**.



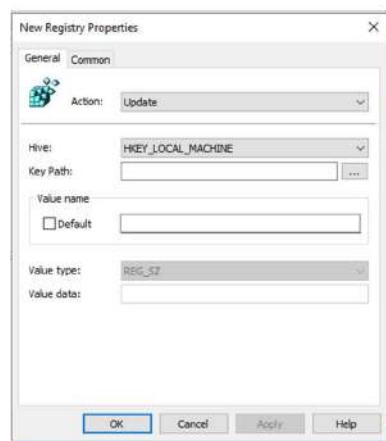
right-click on “Local Admin Remote Login” and choose **Edit**.



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**

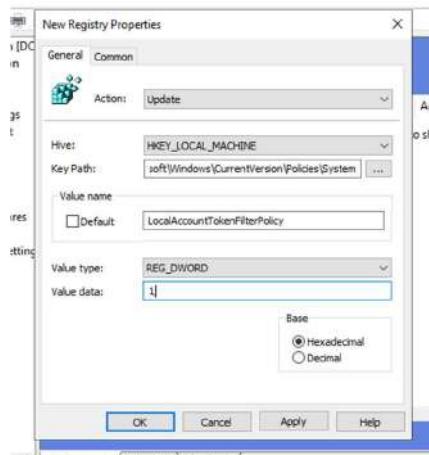
Then enter the following for the remaining fields:

Value name: **LocalAccountTokenFilterPolicy**

Value type: **REG\_DWORD**

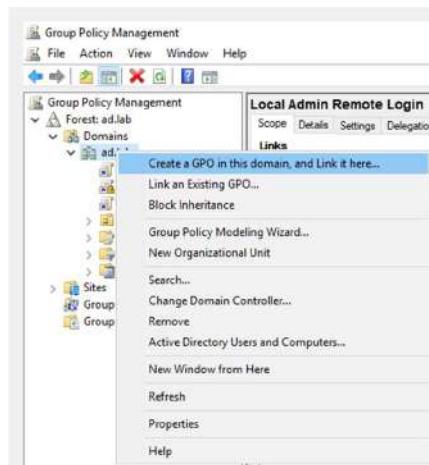
Value data: **1**

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

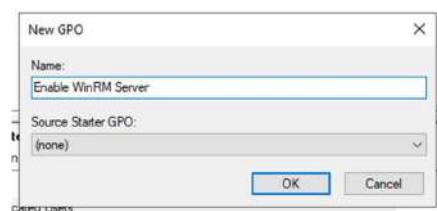


Enable WinRM Server

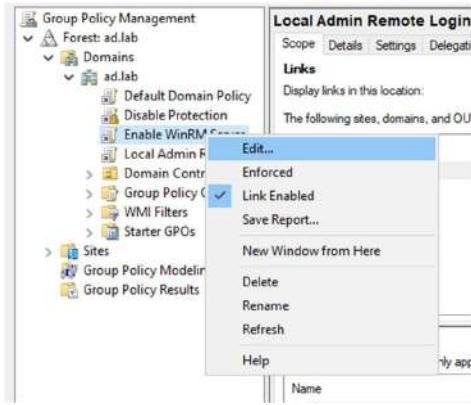
Right-click on the domain name. Select “Create a GPO in the domain and link here”.



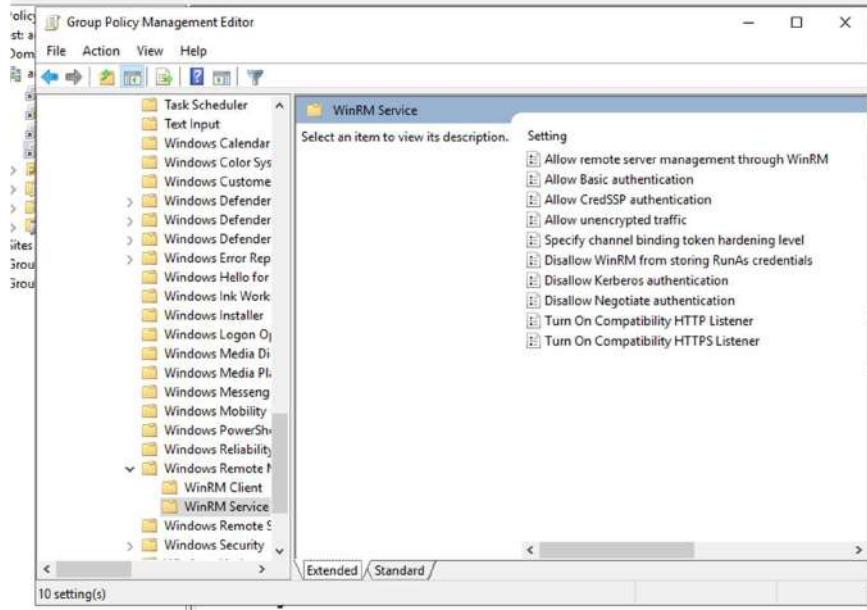
Give the GPO the name **Enable WinRM Server**.



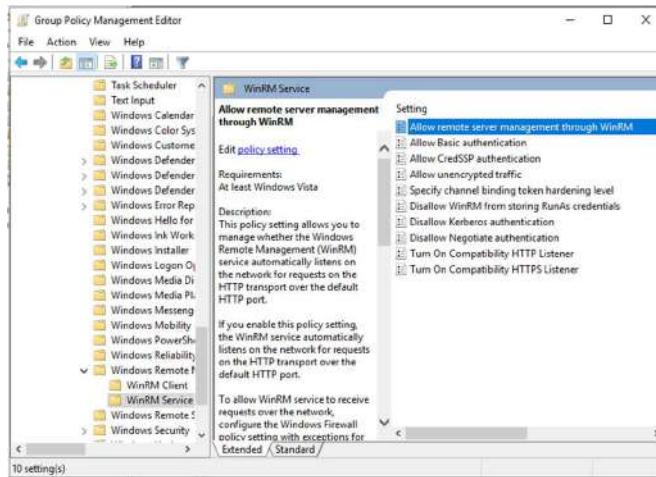
Right-click on “Enable WinRM Server” and choose **Edit**.



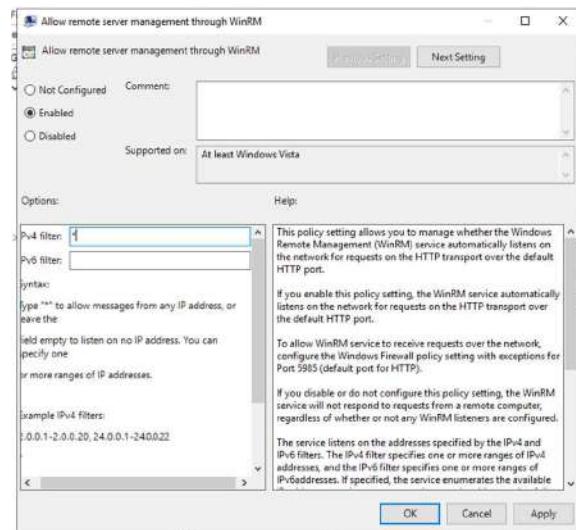
Using the sidebar go to the following folder: **Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Service.**



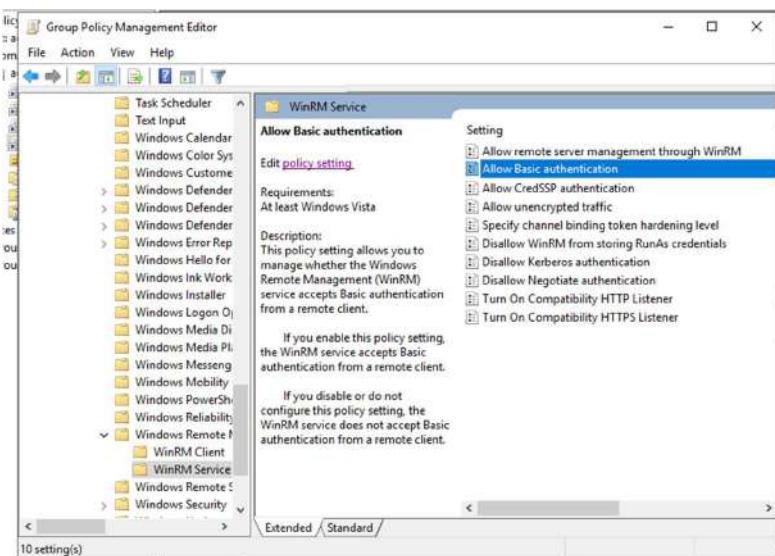
Select “Allow remote server management through WinRM” and then click on “Edit policy settings”.



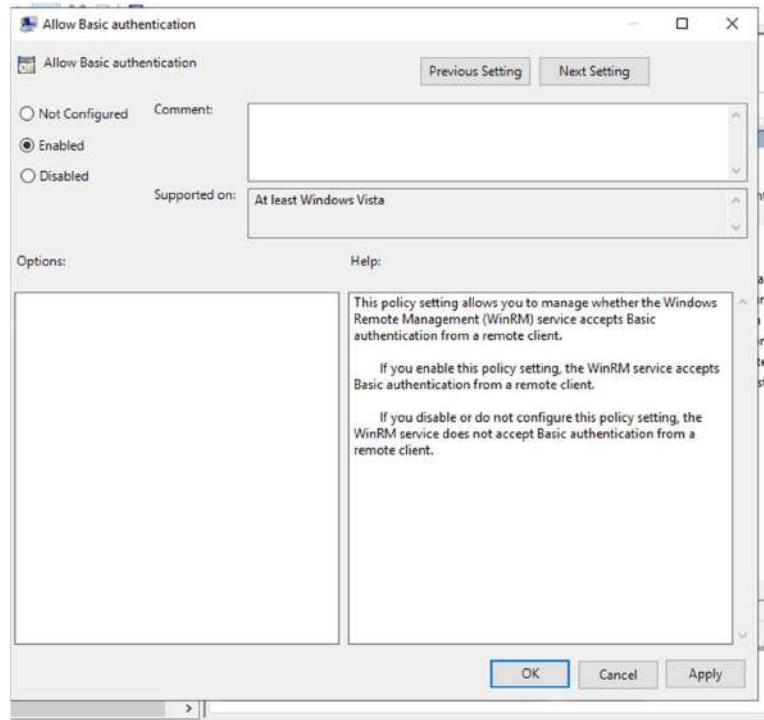
Set the policy to **Enabled**. In the Ipv4 filter field enter **\***. Click on **Apply** then **OK**.



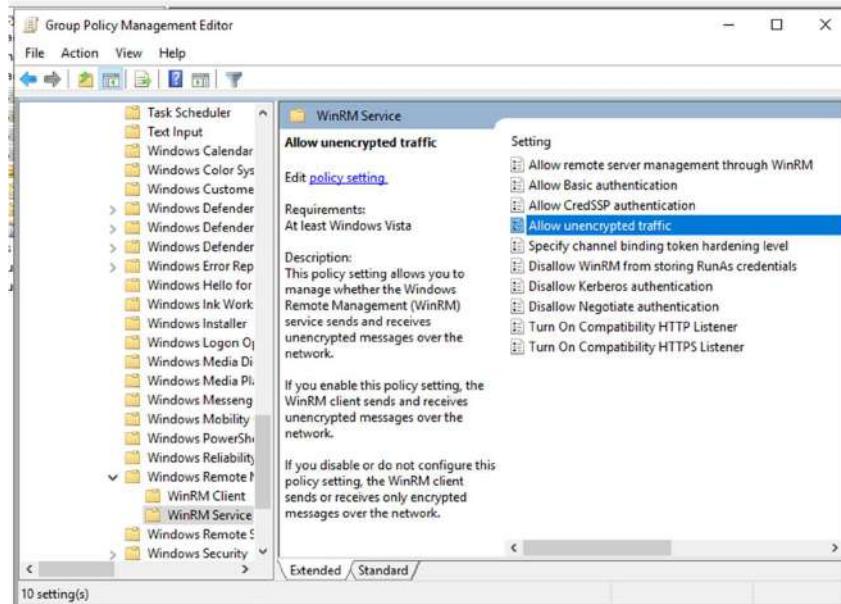
Select “Allow Basic authentication” and click on “Edit policy settings”.



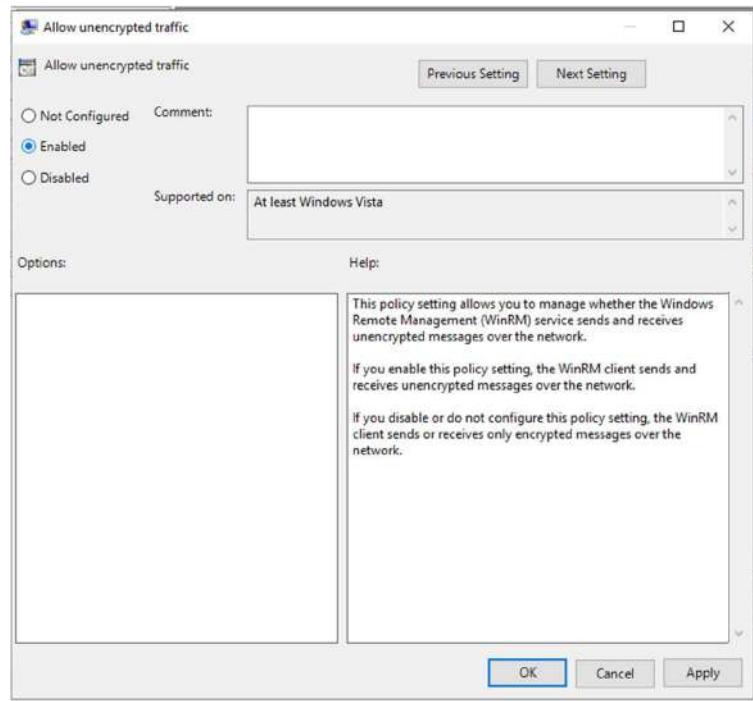
Set the policy to **Enabled**. Click on **Apply** and then **OK**.



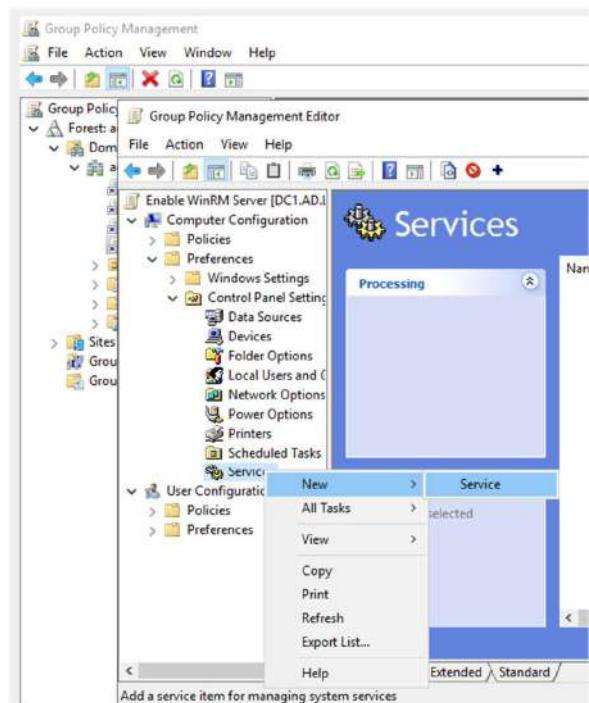
Select “Allow unencrypted traffic” and click on “Edit policy settings”.



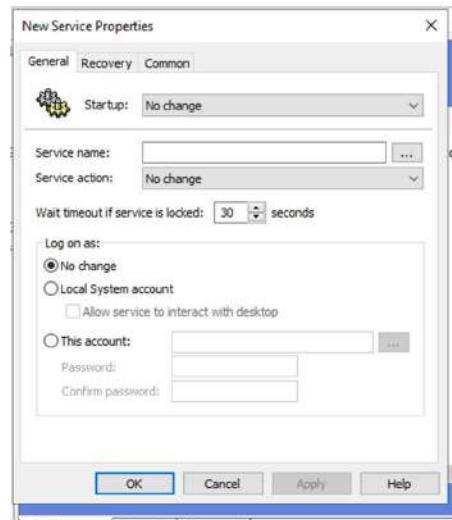
Set the policy to **Enabled**. Click on **Apply** then **OK**.



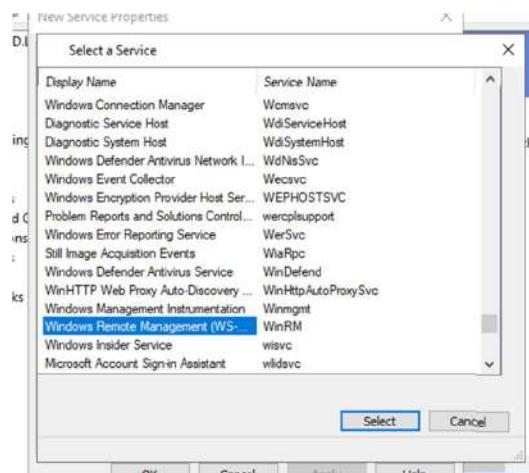
In the sidebar navigate to: **Computer Configuration -> Preferences -> Control Panel Settings**. Right-click on Services and select **New -> Service**.



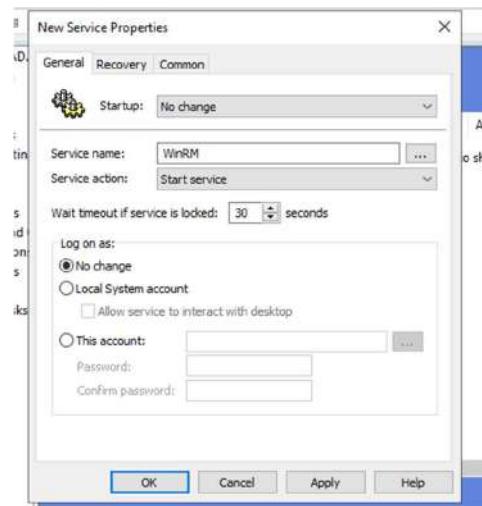
Select Startup to **Automatic**. Use the ... button to select the Server name.



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

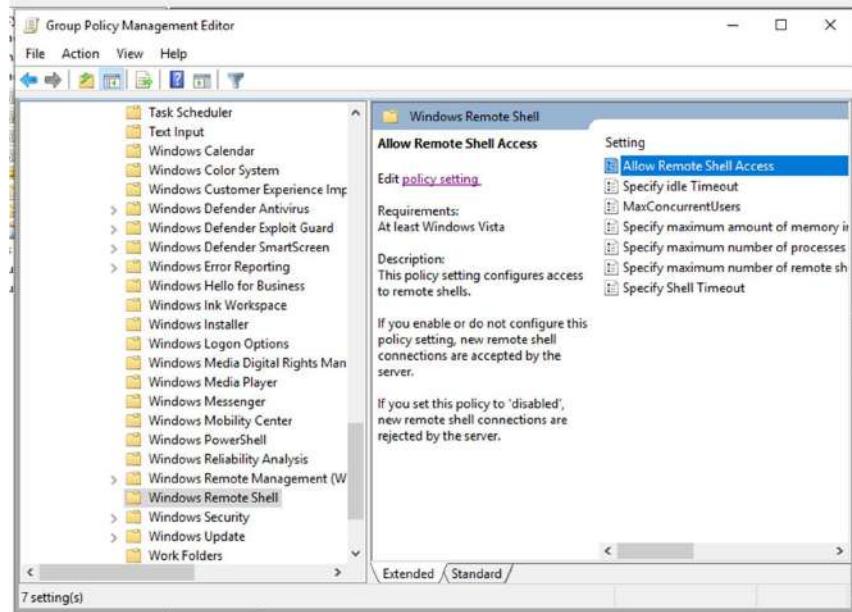


For Service action select **Start service**. Click on **Apply** then **OK**.

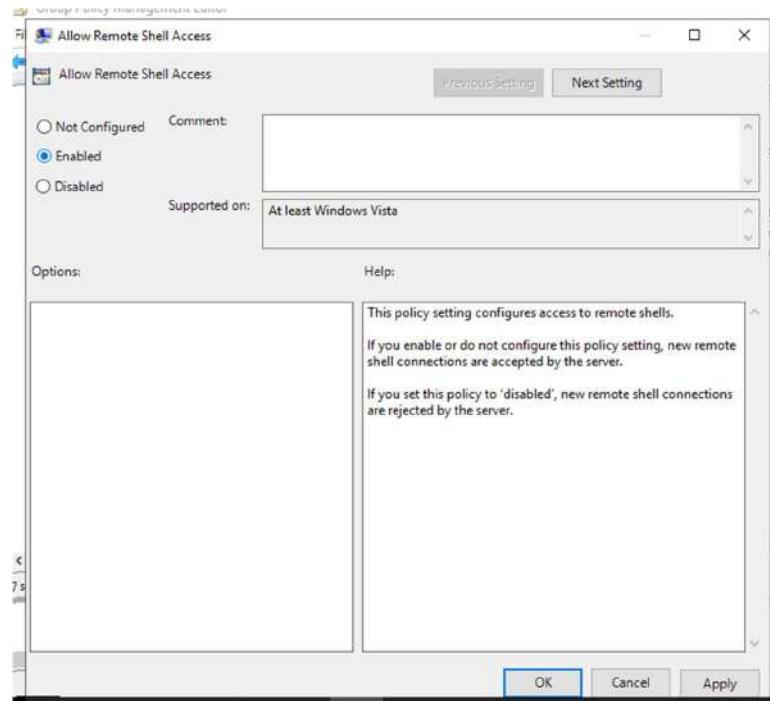


Using the sidebar navigate to the following location: **Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Remote Shell**

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

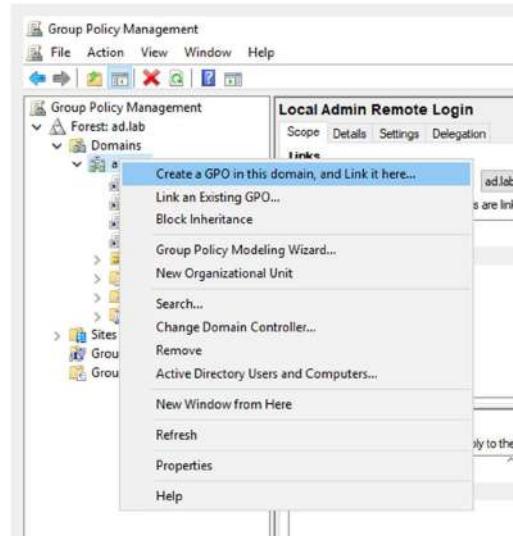


Set the policy to **Enabled**. Click on **Apply** then **OK**. Close the Group Policy Management Editor.



### **Enable RPC (Remote Procedure Call)**

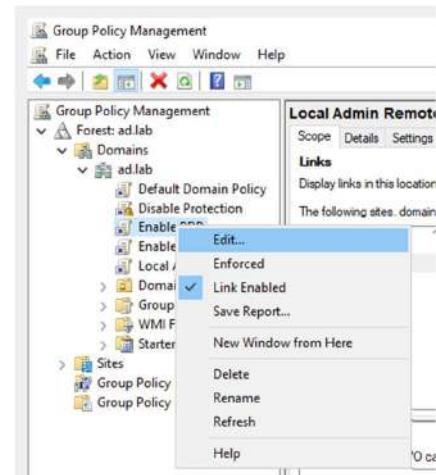
Right-click on the domain name. Select “Create a GPO in the domain and link here”.



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

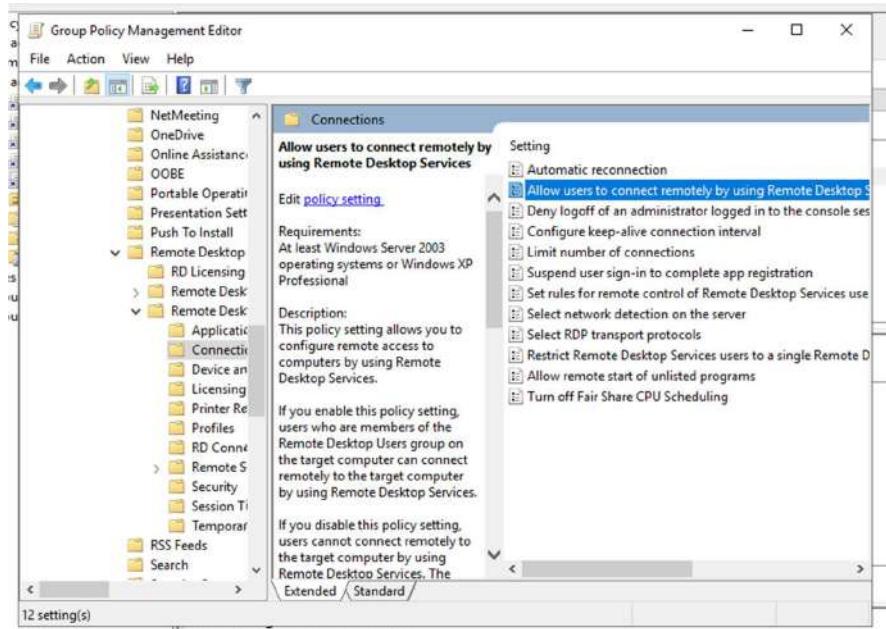


Right-click on "Enable RPC" and select **Edit**.

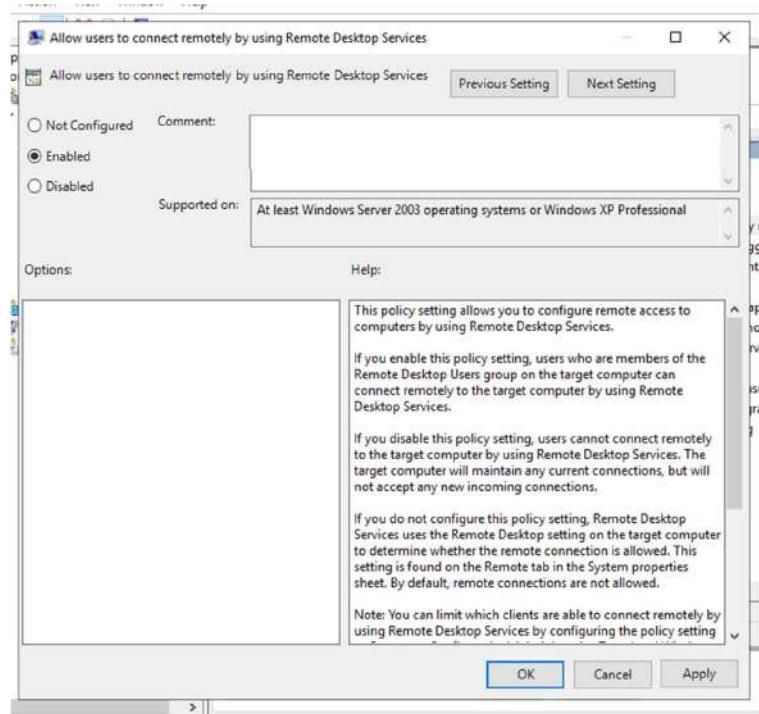


Using the sidebar navigate to the following folder: **Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Connections**.

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

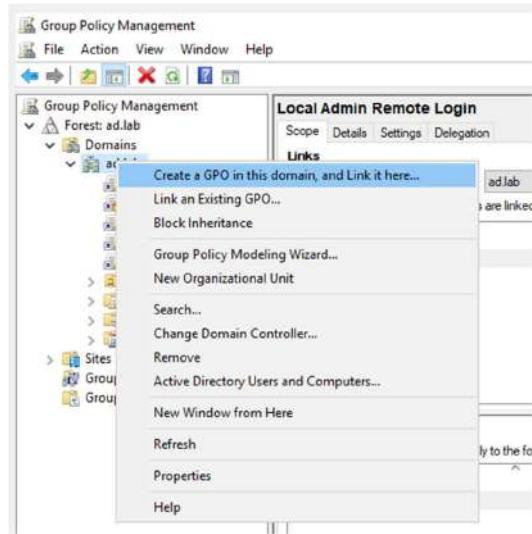


Set the policy to **Enabled**. Click on **Apply** then **OK**. Close Group Policy Management Editor.

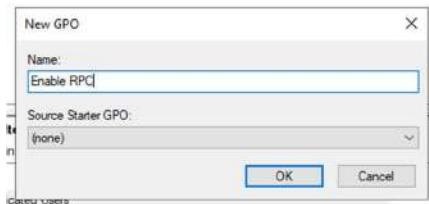


### Enable RPC (Remote Procedure Call)

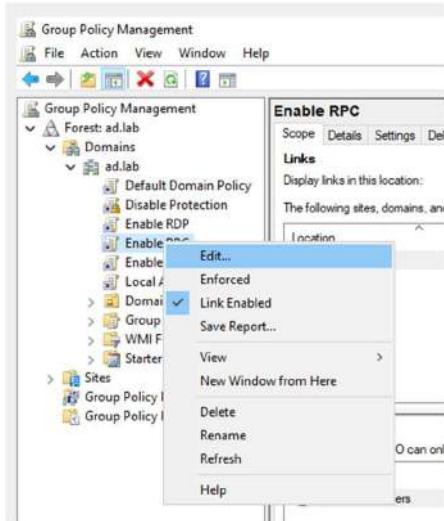
Right-click on the domain name. Select “Create a GPO in the domain and link here”.



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

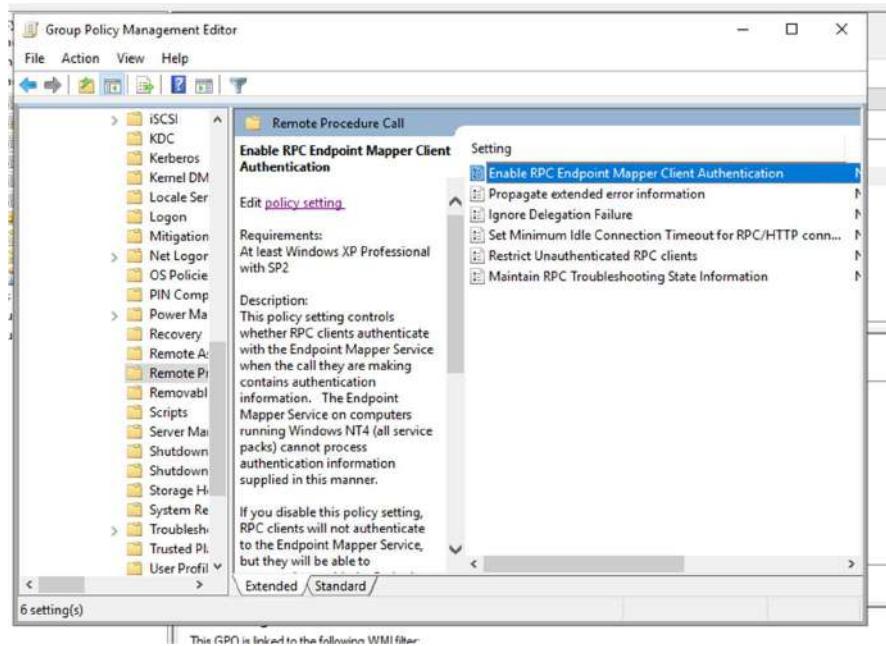


Right-click on "Enable RPC" and select **Edit**.

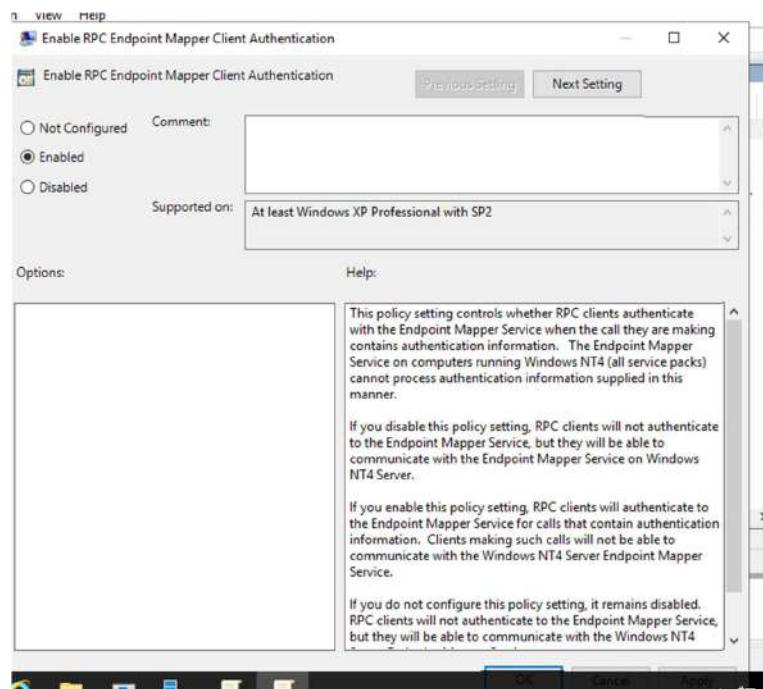


Using the sidebar navigate to the following folder: **Computer Configuration -> Administrative Templates -> System -> Remote Procedure Call**.

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

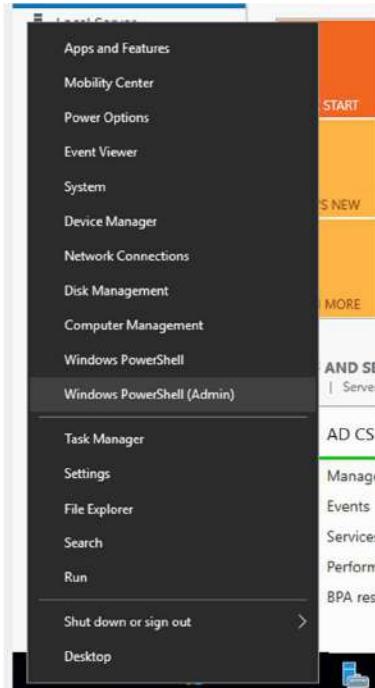


Set the policy to **Enabled**. Click on **Apply** then **OK**. Close Group Policy Management Editor.



Enforce the Domain Policies

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



In the terminal enter the following:

```
gpupdate /force
```

A screenshot of an 'Administrator: Windows PowerShell' terminal window. The command 'gpupdate /force' is entered and executed, resulting in the message 'Computer Policy update has completed successfully.' and 'User Policy update has completed successfully.'.

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](https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise)

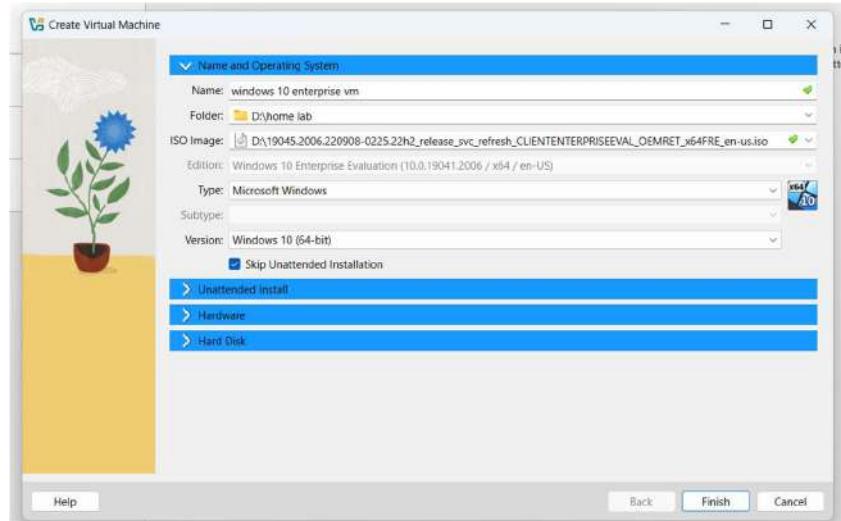
Click on the **64-bit edition** Enterprise ISO download option. The ISO file is ~5GB.

Windows 10 Enterprise VM

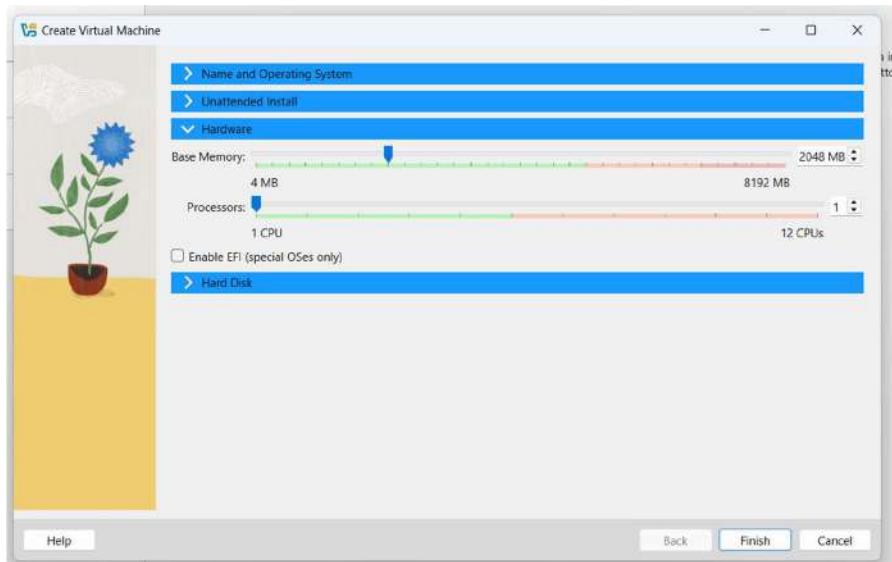
From the VirtualBox sidebar select Tools and then click on **New**.



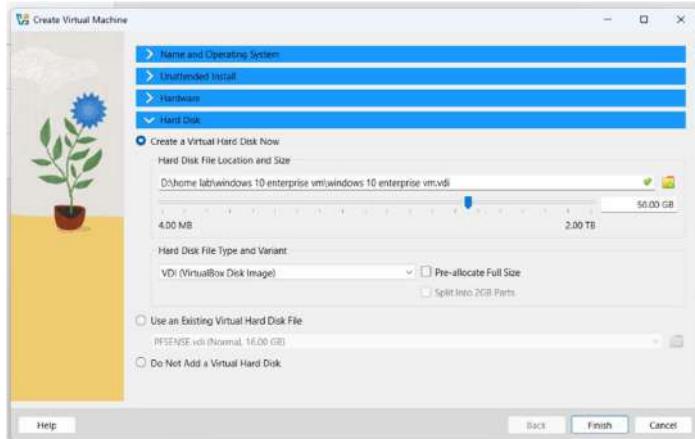
Give the VM a name. Ensure that the Folder option is pointing to the location where all the Home Lab VMs are saved. For the ISO Image option select the Windows 10 Enterprise image. Tick the **Skip Unattended Installation** option. Click on **Next** to continue.



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

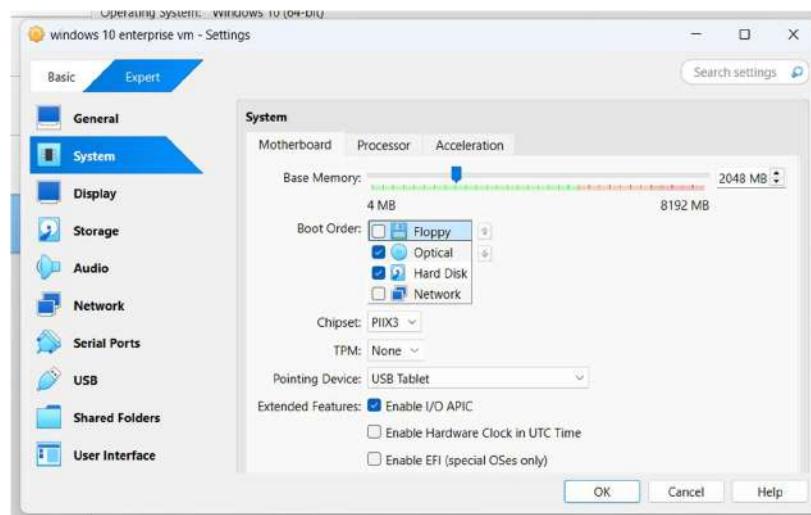


Increase the Hard Disk size to **50GB** and then click on **Finish**.



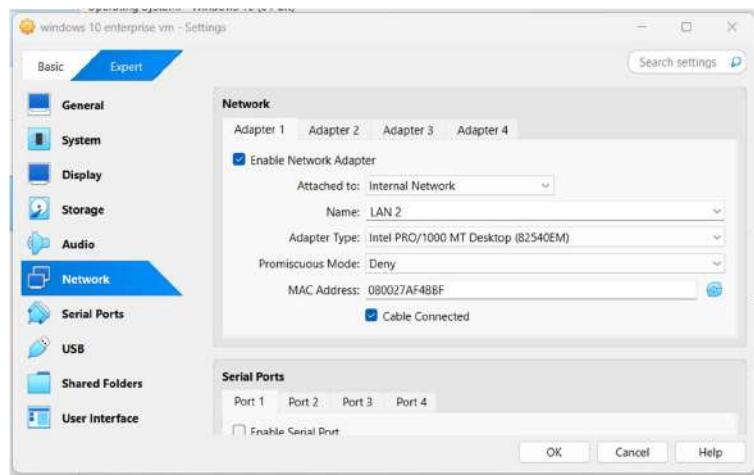
Select Windows 10 Enterprise VM from the sidebar and then from the toolbar choose **Settings**.

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 Attached to field select **Internal Network**.

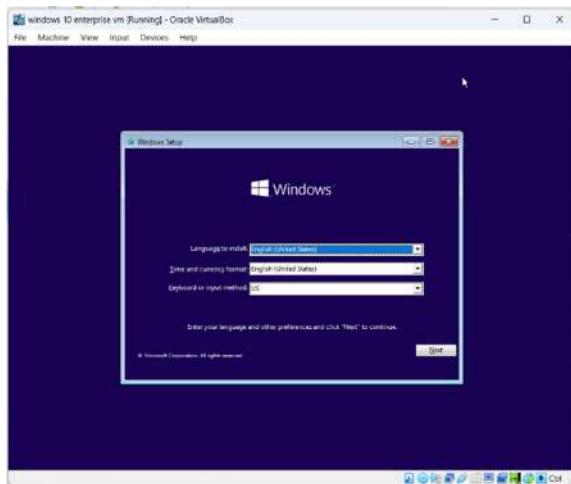
For Name select **LAN 2**. Click on **OK** to save the settings.



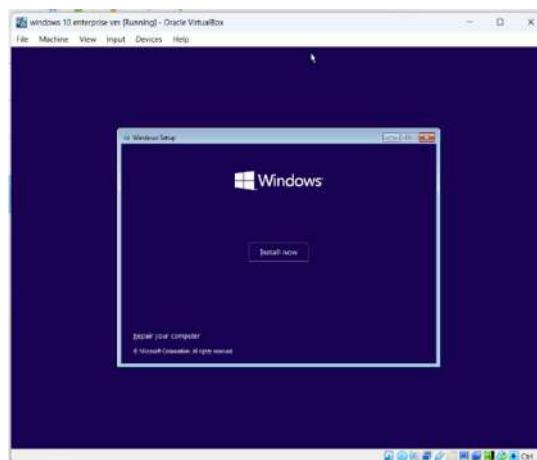
Select Windows 10 Enterprise VM from the sidebar then click on **Start**

## OS Installation

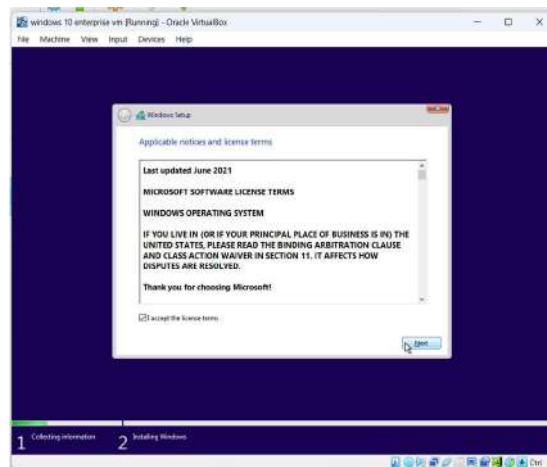
Click on **Next**.



Click on **Install now**.

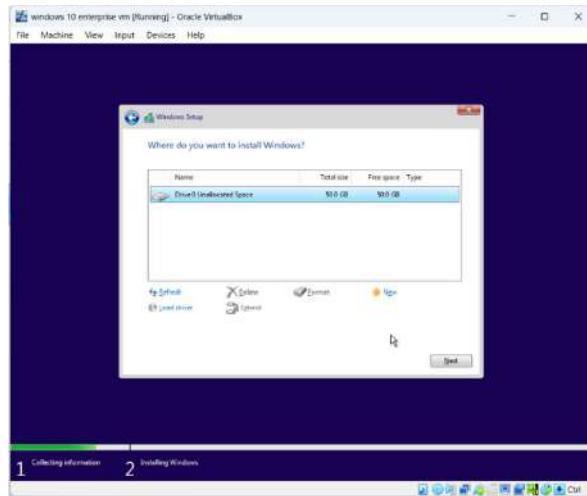


Accept the agreement and then click on **Next**.



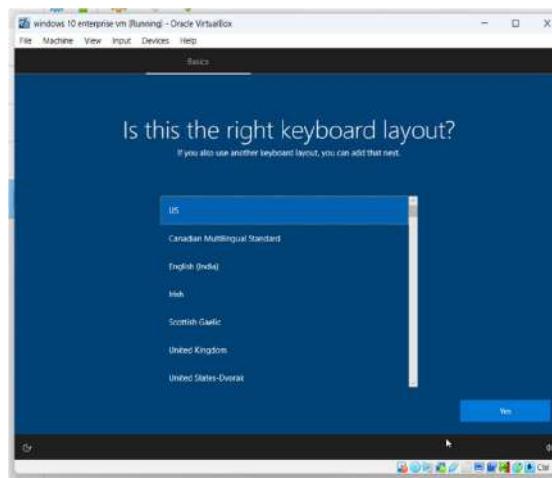
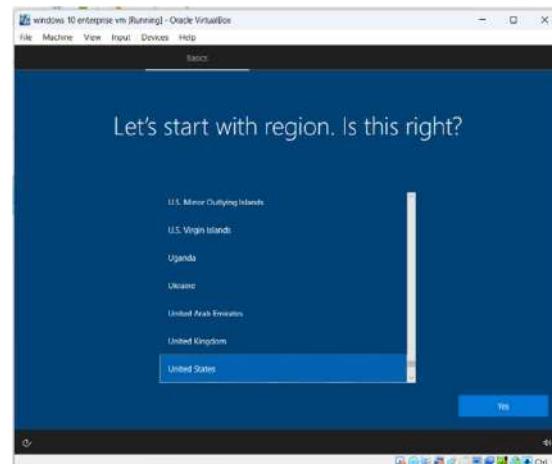
Select “Custom: Install Windows only (advanced)”.

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

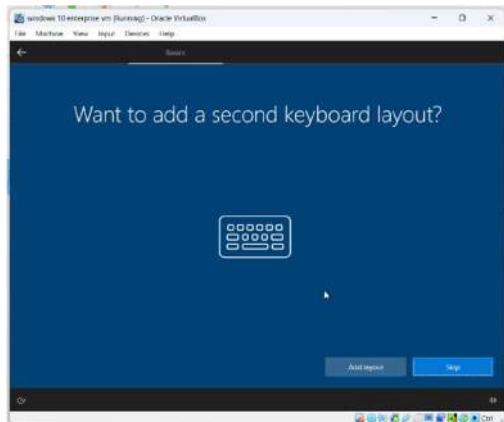


The VM will reboot multiple times during the installation.

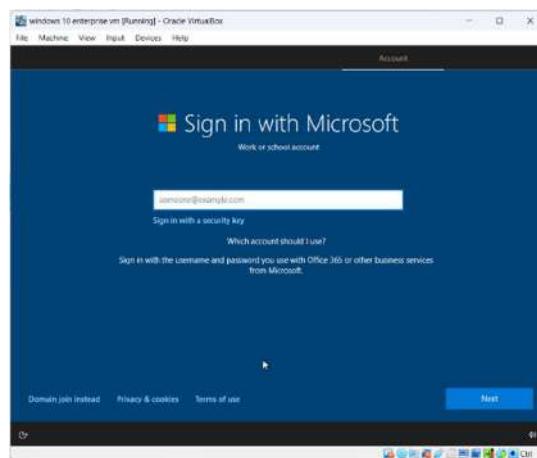
Select your **Region** and **Keyboard Layout**.



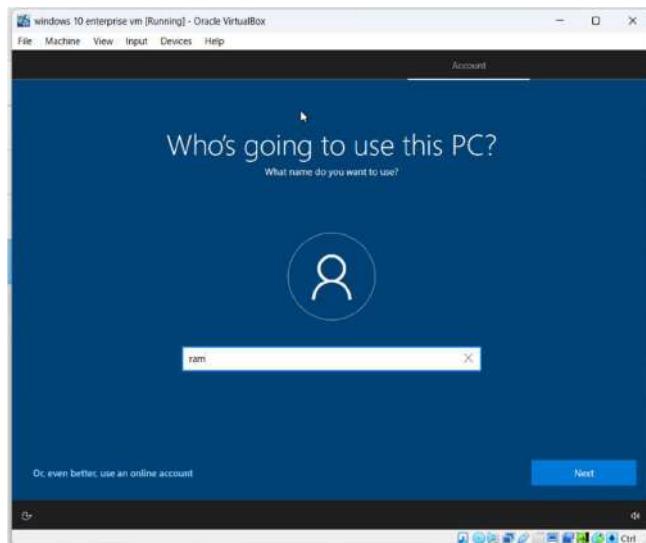
Click on **Skip**.



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

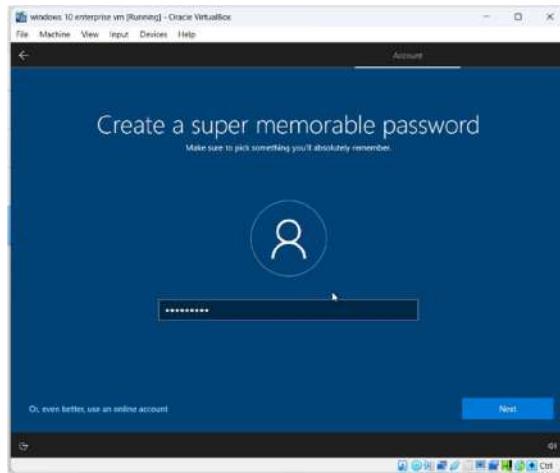


Enter a username and click on **Next**.

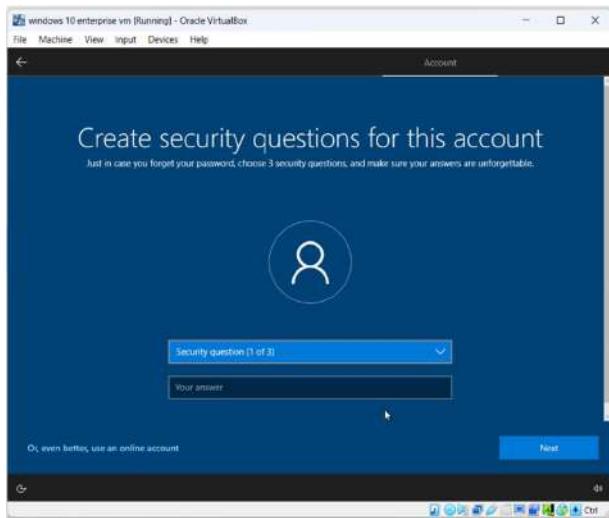


Enter a password and click on **Next**.

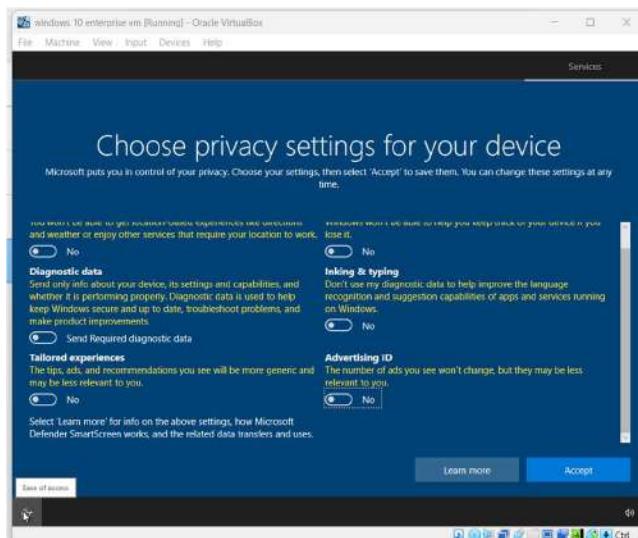
This password can be different from the password that was configured in Active Directory.



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**.



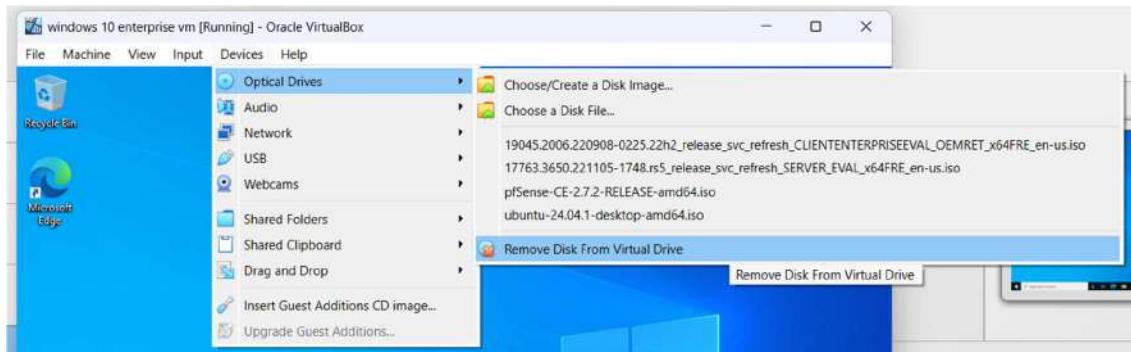
Select **Not now**.



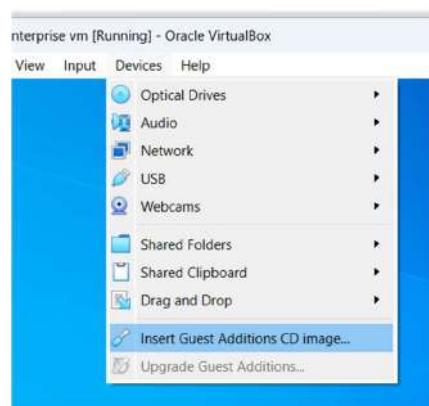
Once on the desktop a prompt to allow internet access should show up click on **Yes**.

#### Guest Additions Installation

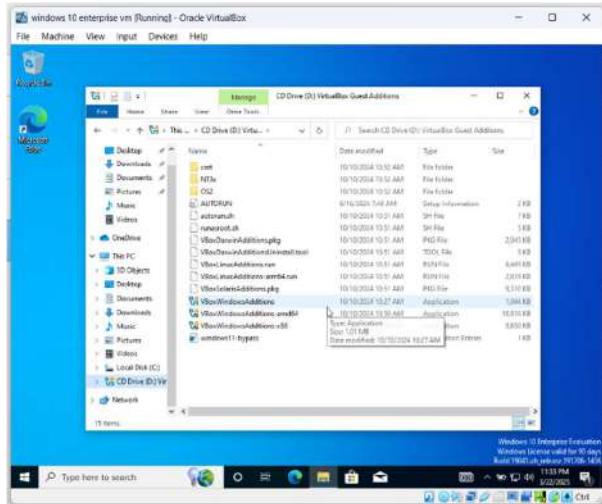
Similar to the Windows 2019 Server VM we need to install [Guest Additions](#) to enable Fullscreen mode. From the VM toolbar select **Devices -> Remove disk for virtual drive**. This will remove the Windows 10 image.



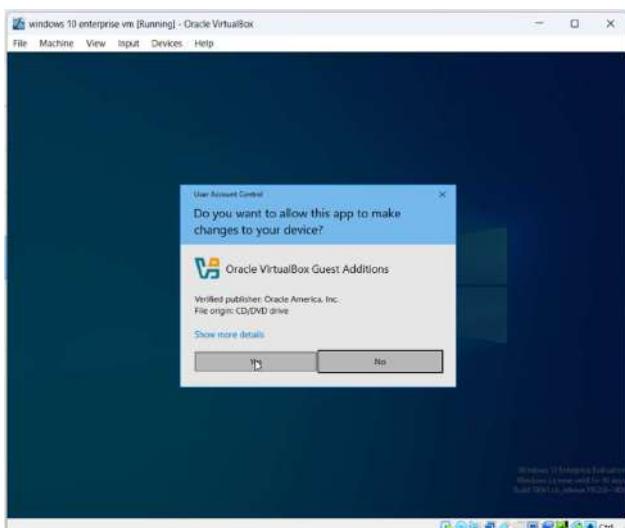
Click on **Devices -> Insert Guest Additions CD image**.



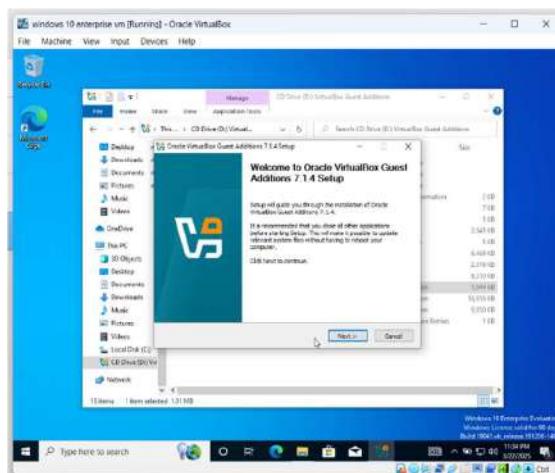
Open File Explorer. Once the disk has loaded from the sidebar select the disk drive. Double-click **VboxWindowsAdditions** to start the installer.



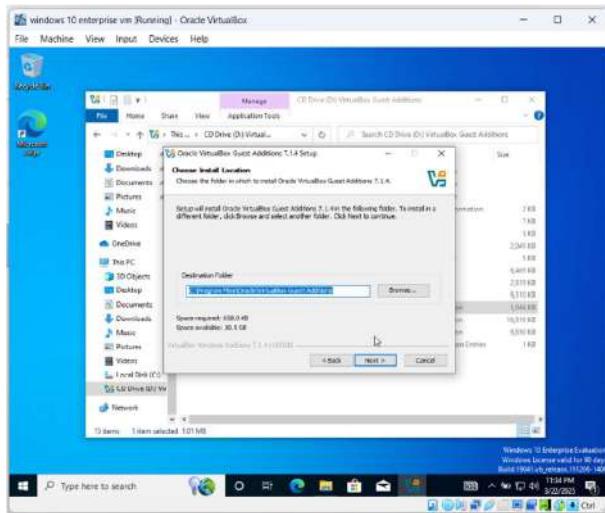
Click **Next**.



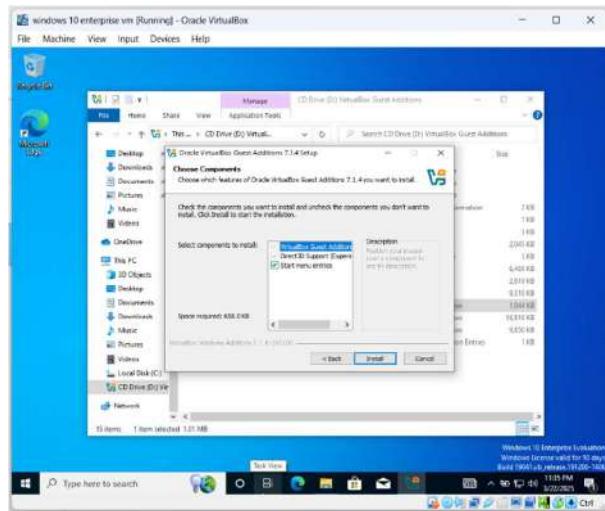
Click **Next**.



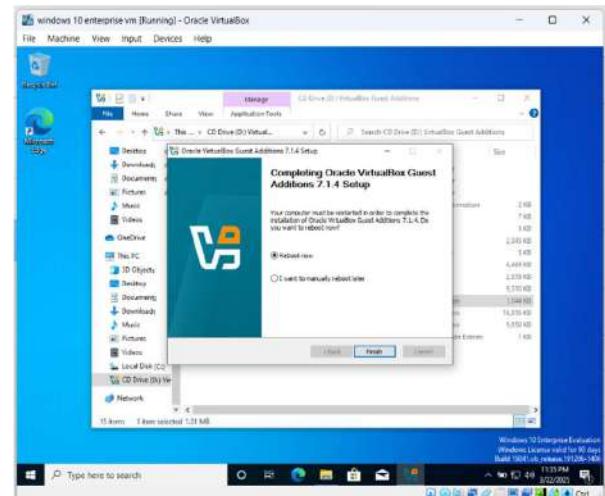
Click **Next**.



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

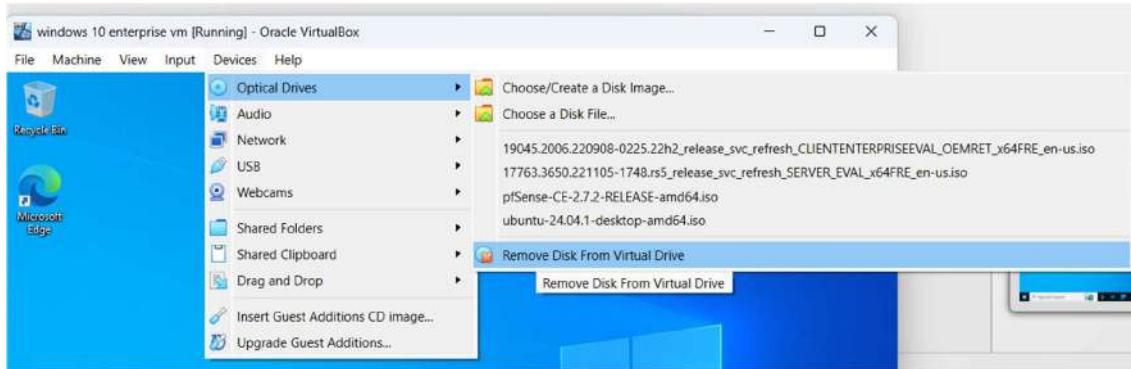


Select “Reboot now” and then click on **Finish**. The VM will reboot.



Login into the system.

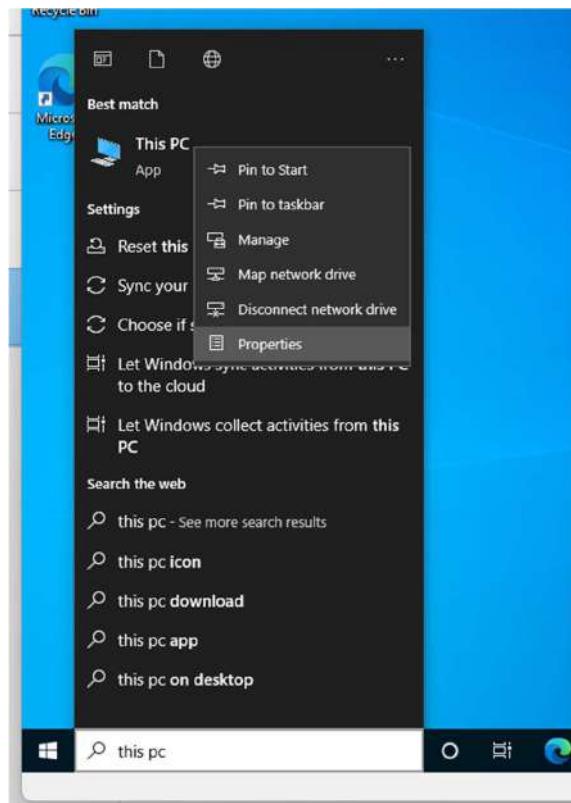
From the toolbar select **Optical Devices -> Remove disk from virtual drive** to remove the Guest Additions image.



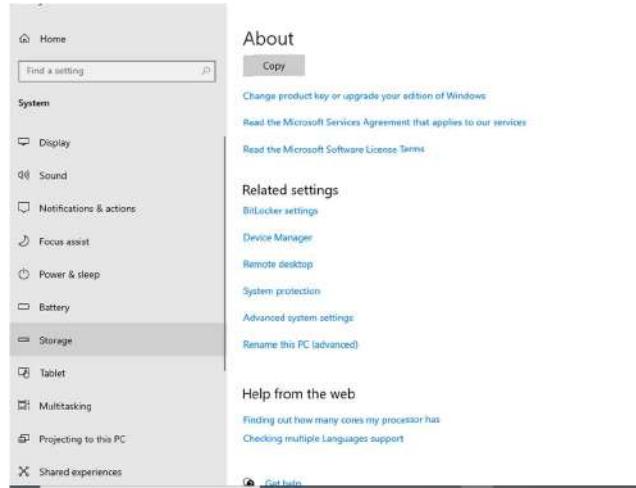
Use the shortcut **Ctrl+F** to enter Fullscreen mode. Use the same key to exit Fullscreen. The VM should automatically scale to fit the window size.

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

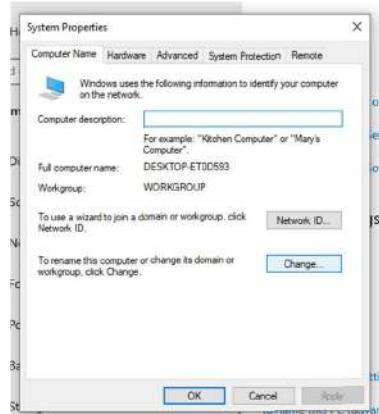
Click on the Search Bar and search for “This PC”. Right-click on it and select **Properties**.



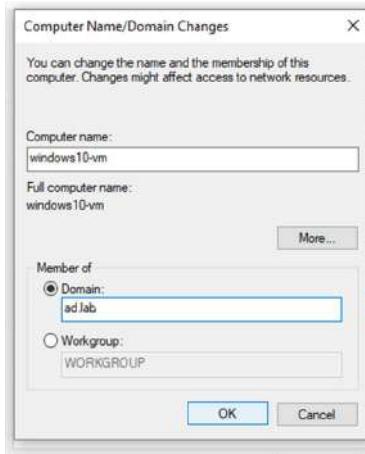
Click on **Advanced system settings**.



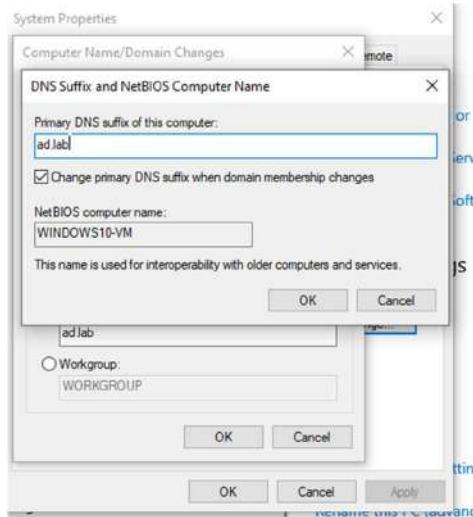
Select the “Computer Name” tab and click on **Change**.



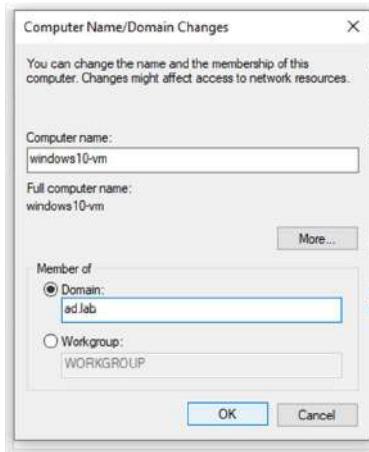
In the Computer name field enter a name that can be used to easily identify this VM. In the Member of section select **Domain** and enter the name of the AD domain (in my case **ad.lab**). Then click on **More**.



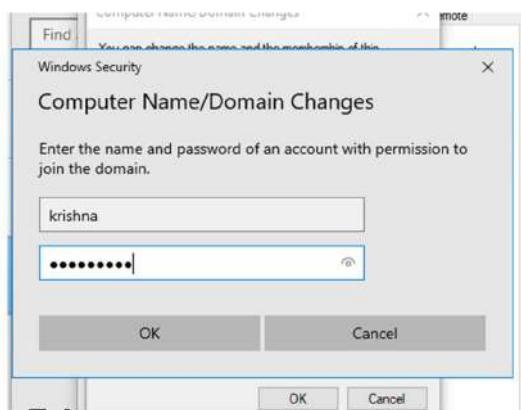
In the “Primary DNS suffix of this computer” field enter the domain name. Click on **OK**.



Click on **OK**.



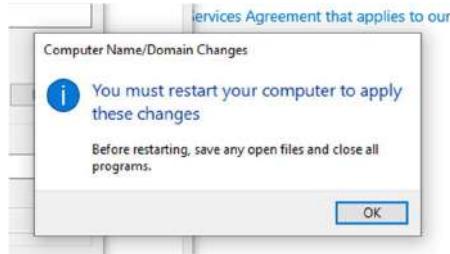
Now a popup should appear. Enter the login name and password of the Domain Admin and click on **OK**.



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

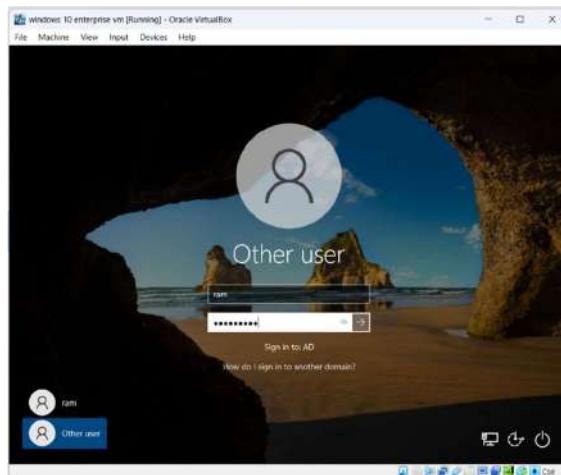


The device needs to be rebooted to apply the domain-specific settings. Click on **OK** to continue.

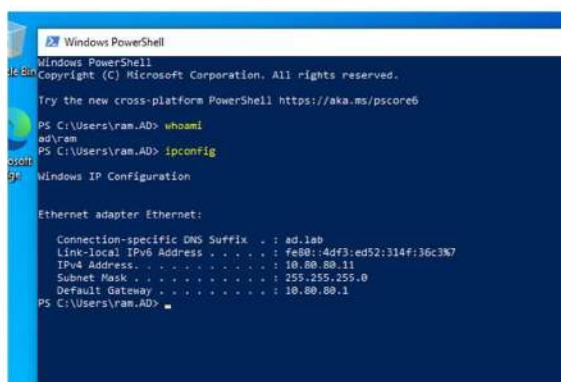


Click on "Restart Now".

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**.

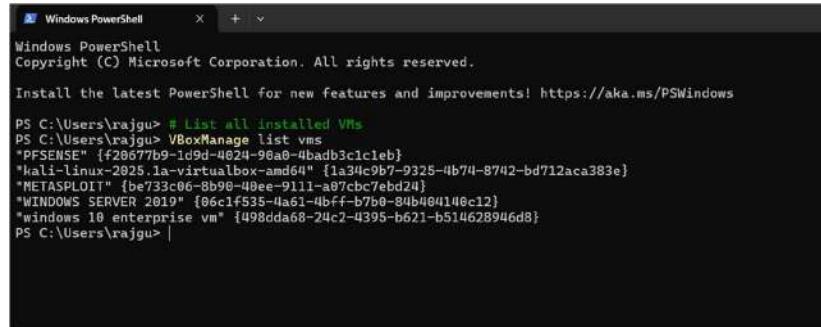
In the top window select the variable named “Path” and then click on **Edit**.

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**



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\rajuu> # List all installed VMs
PS C:\Users\rajuu> VBoxManage list vms
"PFSENSE" {20677b9-1d9d-4024-90a0-4badb3c1c1eb}
"Kali-linux-2025.1a-virtualbox-amd64" {1a34c9b7-9325-4b74-8742-bd712aca383e}
"METASPLOIT" {be733c06-8b90-40ee-9111-a87cbc7ebd24}
"WINDOWS SERVER 2019" {06c1f535-4a61-4bff-b7b0-80b404146c12}
"windows 10 enterprise vm" {498ddaa8-24c2-4395-b621-b514628946d8}
PS C:\Users\rajuu> |
```

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"**

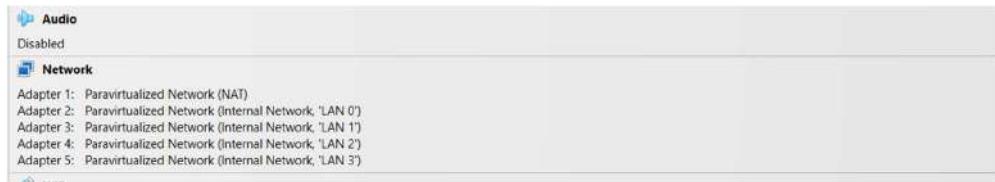
Network Int connected by Cable: **VBoxManage modifyvm "PFSENSE" --cableconnected5 on**

```

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

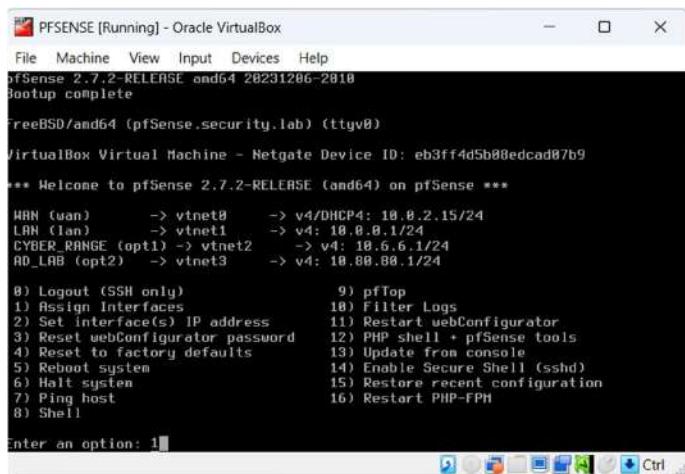
```

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



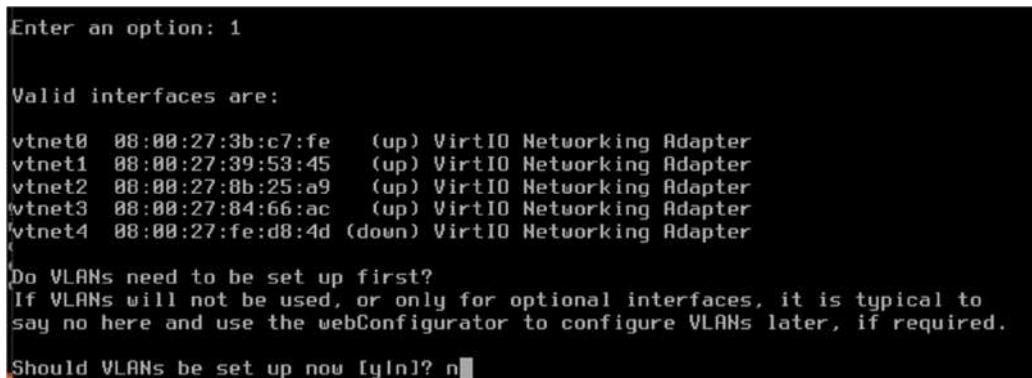
## Enabling the Interface

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.

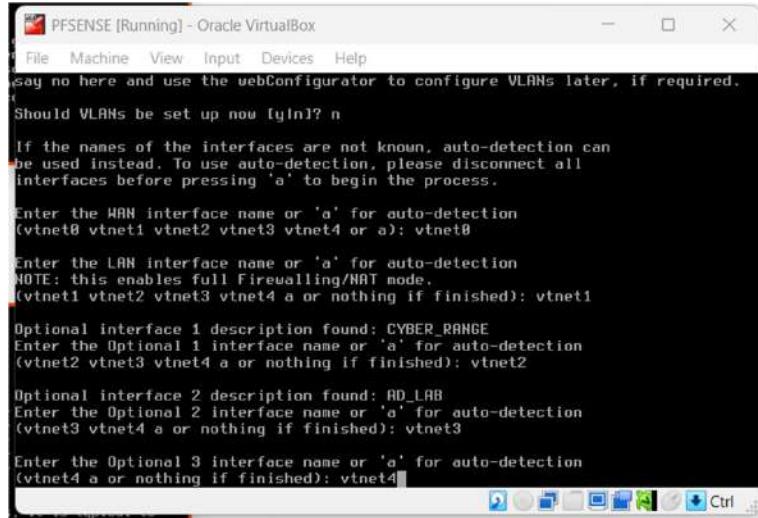


Enter 1 to select “Assign Interfaces”.

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**



```
File Machine View Input Devices Help
Say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y/n]? n

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

Enter the WAN interface name or 'a' for auto-detection
(vtnet0 vtnet1 vtnet2 vtnet3 vtnet4 or a): vtnet0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtnet1 vtnet2 vtnet3 vtnet4 a or nothing if finished): vtnet1

Optional interface 1 description found: CYBER_RANGE
Enter the Optional 1 interface name or 'a' for auto-detection
(vtnet2 vtnet3 vtnet4 a or nothing if finished): vtnet2

Optional interface 2 description found: AD_LAB
Enter the Optional 2 interface name or 'a' for auto-detection
(vtnet3 vtnet4 a or nothing if finished): vtnet3

Enter the Optional 3 interface name or 'a' for auto-detection
(vtnet4 a or nothing if finished): vtnet4
```

Do you want to proceed?: y

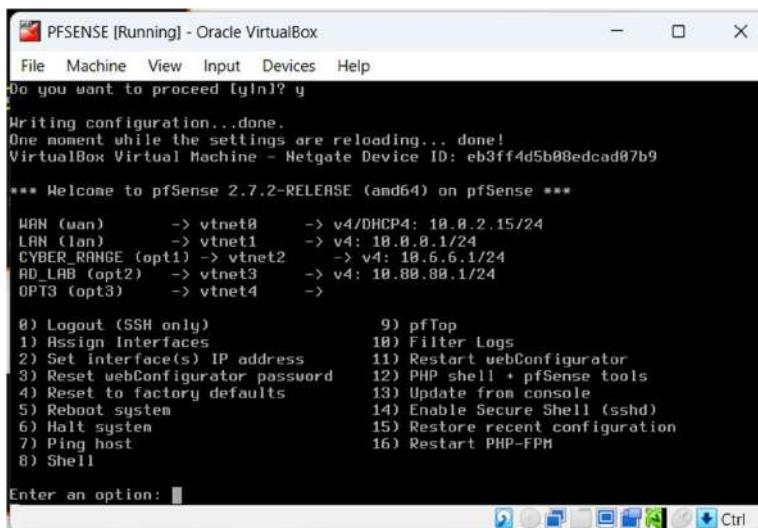


```
The interfaces will be assigned as follows:

WAN -> vtnet0
LAN -> vtnet1
OPT1 -> vtnet2
OPT2 -> vtnet3
OPT3 -> vtnet4

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

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



```
File Machine View Input Devices Help
Do you want to proceed [y/n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
VirtualBox Virtual Machine - Netgate Device ID: eb3ff4d5b08edcad07b9

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

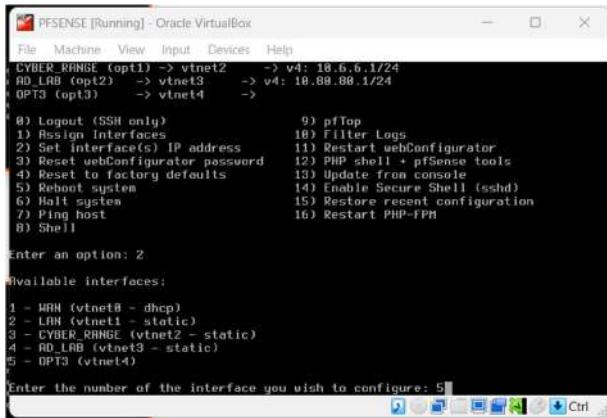
WAN (wan)      -> vtnet0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet1      -> v4: 10.0.0.1/24
CYBER_RANGE (opt1) -> vtnet2      -> v4: 10.6.6.1/24
AD_LAB (opt2)  -> vtnet3      -> v4: 10.0.0.1/24
OPT3 (opt3)    -> vtnet4      ->

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

Enter an option: 1
```

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**

```
Configure IPv4 address OPT3 interface via DHCP? (y/n) n
Enter the new OPT3 IPv4 address. Press <ENTER> for none:
> 10.99.99.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0 = 16
      255.0.0.0 = 8
>

Enter the new OPT3 IPv4 subnet bit count (1 to 32):
> 24
```

```
For a WAN, enter the new OPT3 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

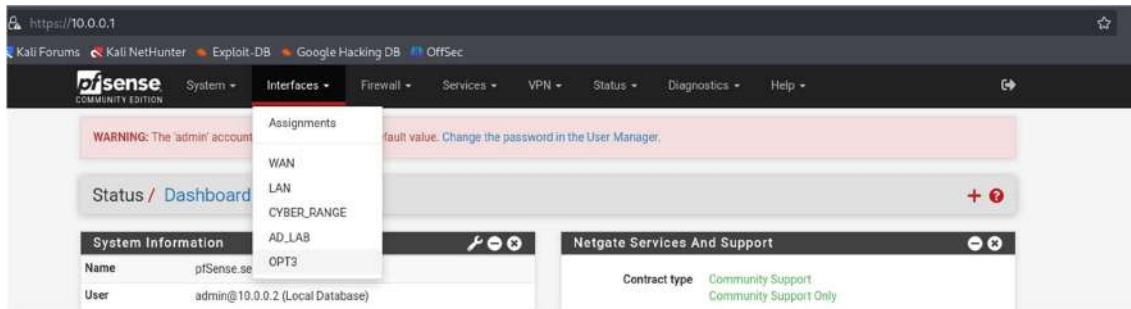
Configure IPv6 address OPT3 interface via DHCP6? (y/n) n
Enter the new OPT3 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT3? (y/n) 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
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

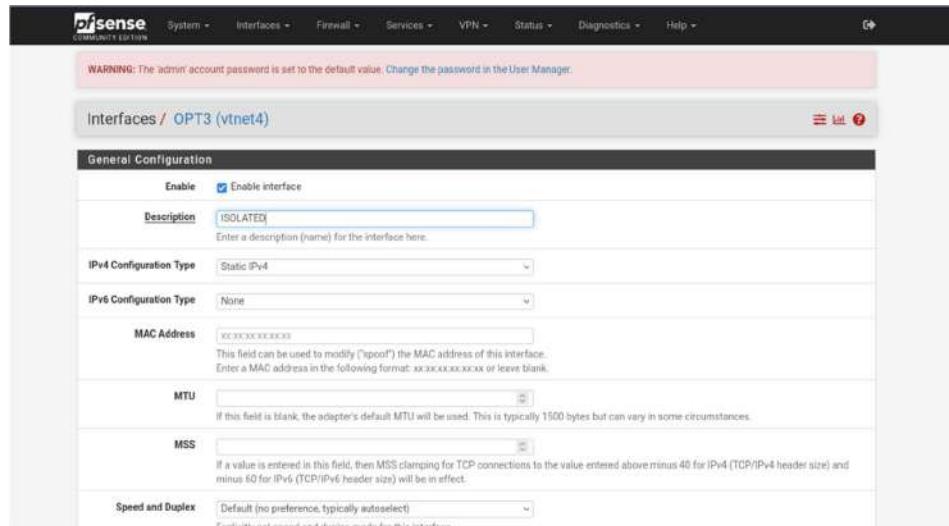
Now interface OPT3 will have an IP address.

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



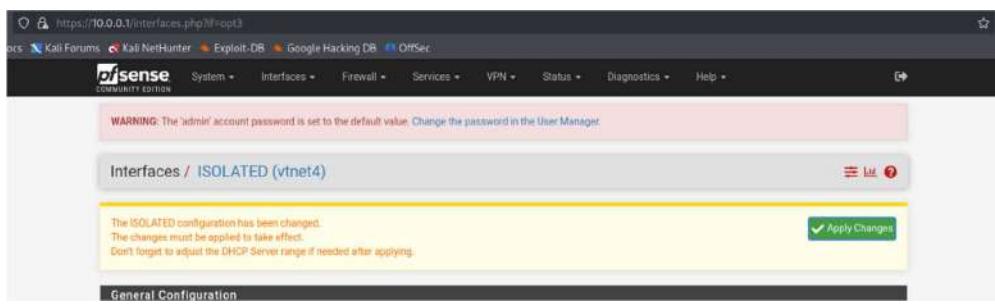
The screenshot shows the pfSense web interface at <https://10.0.0.1>. The navigation bar includes links for Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main menu has options for System, Firewall, Services, VPN, Status, Diagnostics, and Help. The 'Interfaces' menu is open, showing sub-options: Assignments, WAN, LAN, CYBER\_RANGE, AD\_LAB, and OPT3. The 'OPT3' option is highlighted. The left sidebar shows 'System Information' with 'Name: pfSense' and 'User: admin@10.0.0.2 (Local Database)'. The right sidebar shows 'Netgate Services And Support' with 'Contract type: Community Support' and 'Community Support Only'.

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



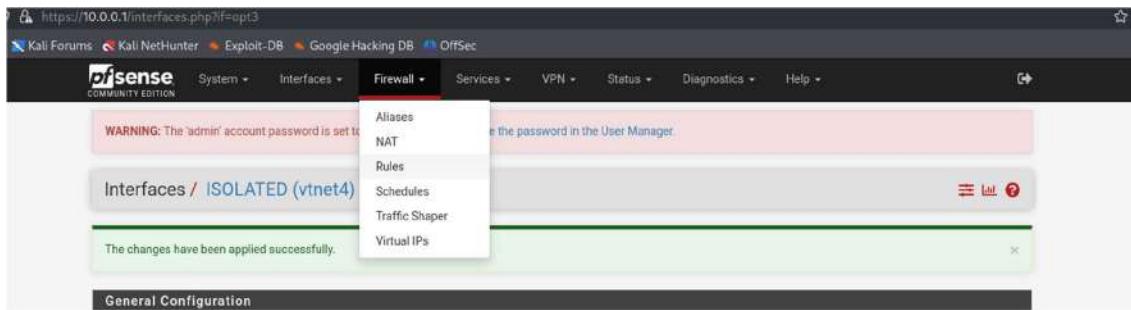
The screenshot shows the 'Interfaces / OPT3 (vtnet4)' configuration page. The 'General Configuration' section includes fields for 'Enable' (checked), 'Description' (set to 'ISOLATED'), 'IPv4 Configuration Type' (set to 'Static IPv4'), 'IPv6 Configuration Type' (set to 'None'), 'MAC Address' (set to '00:0C:29:00:00:00'), 'MTU' (set to '1500'), 'MSS' (set to '60'), and 'Speed and Duplex' (set to 'Default (no preference, typically autoselect)').

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

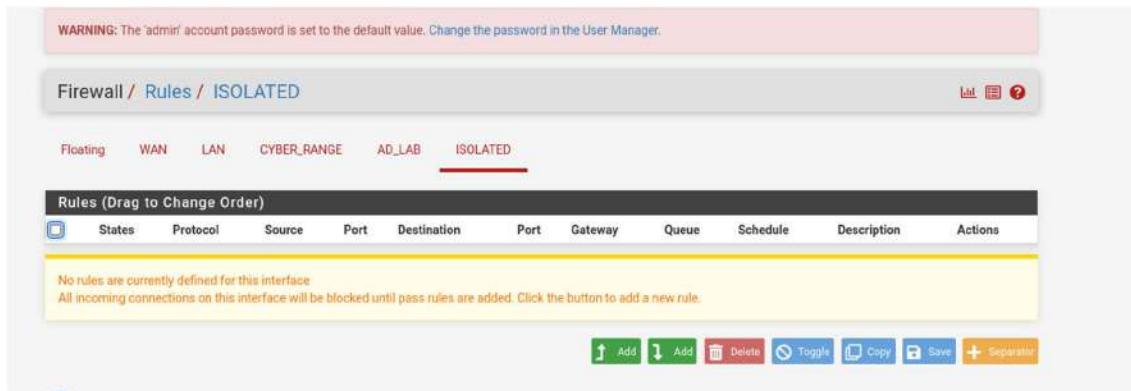


The screenshot shows the 'Interfaces / ISOLATED (vtnet4)' configuration page. A message box displays: 'The ISOLATED configuration has been changed. The changes must be applied to take effect. Don't forget to adjust the DHCP server range if needed after applying.' A green 'Apply Changes' button is visible in the bottom right corner.

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.

The screenshot shows the pfSense firewall configuration interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The current page is 'Firewall / Rules / ISOLATED'. A message at the top states: 'WARNING: The "admin" account password is set to the default value. Change the password in the User Manager.' Below this, a message says: 'The firewall rule configuration has been changed. The changes must be applied for them to take effect.' A green 'Apply Changes' button is visible. The main content area shows a table of rules with one entry: '0/0 B' (Protocol: IPv4+6, Source: ISOLATED subnets, Destination: \*, Port: \*, Gateway: \*, Queue: none, Description: block access to everything). Below the table are several action buttons: Add, Add, Delete, Toggle, Copy, Save, and a plus sign for more options. The 'ISOLATED' tab is selected in the navigation bar.

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

The screenshot shows the pfSense diagnostics interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The current page is 'Diagnostics / Reboot'. A message at the top states: 'WARNING: The "admin" account password is set to the default value. Change the password in the User Manager.' Below this, a message says: 'The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.' The main content area shows a 'Select reboot method' form with a dropdown menu set to 'Normal reboot'. A note below the dropdown says: 'Select "Normal reboot" to reboot the system immediately, or "Reroot" to stop processes, remount disks and re-run startup sequence.' A blue 'Submit' button is at the bottom. The right side of the screen is a sidebar with a list of diagnostic tools: ARP Table, Authentication, Backup & Restore, Command Prompt, DNS Lookup, Edit File, Factory Defaults, Halt System, Limiter Info, NDP Table, Packet Capture, pfBfns, pfTop, Ping, Reroot, Routes, S.M.A.R.T. Status, Sockets, States, States Summary, System Activity, Tables, Test Port, and Traceroute. The 'Reboot' tool is highlighted in the sidebar.

Click on **Submit**.

The screenshot shows the pfSense diagnostics interface after a submission. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The current page is 'Diagnostics / Reboot'. A message at the top states: 'WARNING: The "admin" account password is set to the default value. Change the password in the User Manager.' Below this, a message says: 'The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.' The main content area shows a 'Select reboot method' form with a dropdown menu set to 'Normal reboot'. A note below the dropdown says: 'Select "Normal reboot" to reboot the system immediately, or "Reroot" to stop processes, remount disks and re-run startup sequence.' A blue 'Submit' button is at the bottom. The right side of the screen is a sidebar with a list of diagnostic tools: ARP Table, Authentication, Backup & Restore, Command Prompt, DNS Lookup, Edit File, Factory Defaults, Halt System, Limiter Info, NDP Table, Packet Capture, pfBfns, pfTop, Ping, Reroot, Routes, S.M.A.R.T. Status, Sockets, States, States Summary, System Activity, Tables, Test Port, and Traceroute. The 'Reboot' tool is highlighted in the sidebar.

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

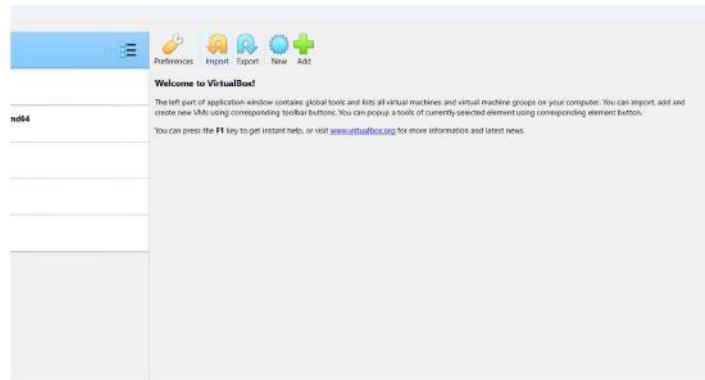
## Windows ISO Download

Go to the following URL: [Windows 10 Enterprise | Microsoft Evaluation Center](https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise)

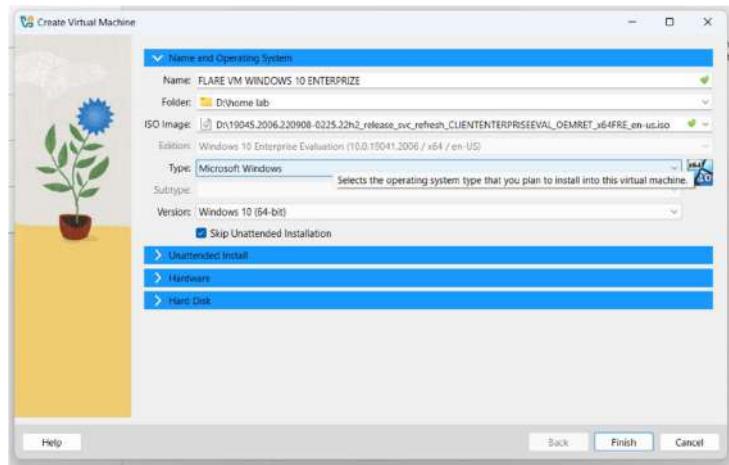
Click on the 64-bit edition Enterprise ISO download option. The ISO file is ~5GB.

## Creating the VM

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



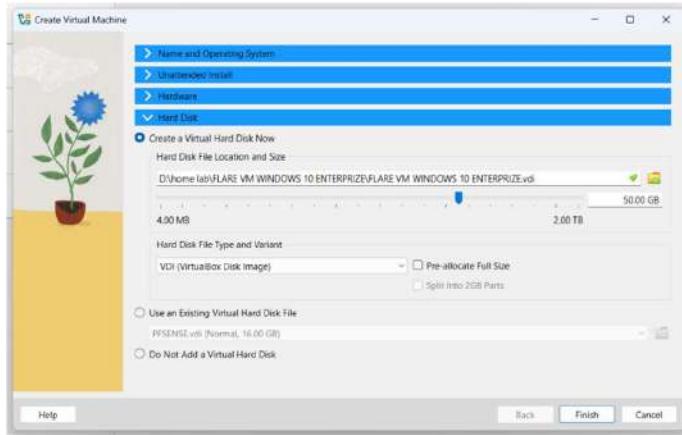
Give the VM a name. Select the downloaded Windows 10 ISO Image. Check “Skip Unattended Installation”. Then click on **Next**.



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

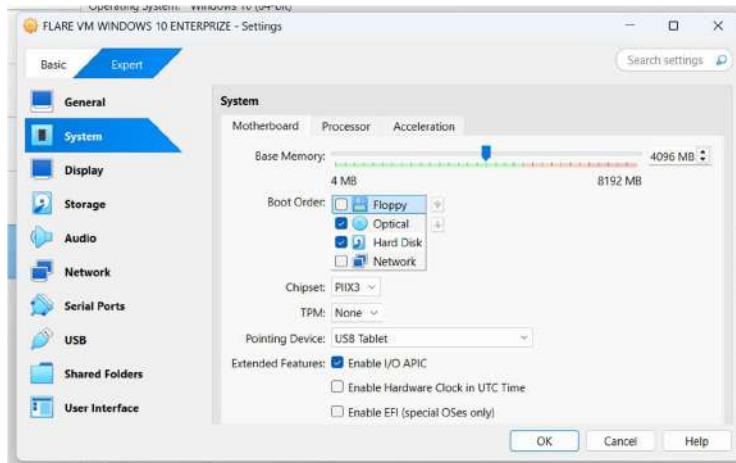


Increase the **Drive Size** to **50GB** and click on **Finish**.

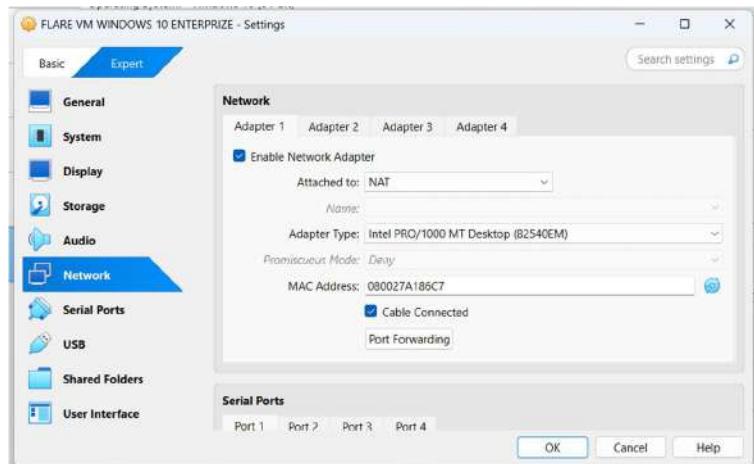


Select the VM then from the toolbar select **Settings**.

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



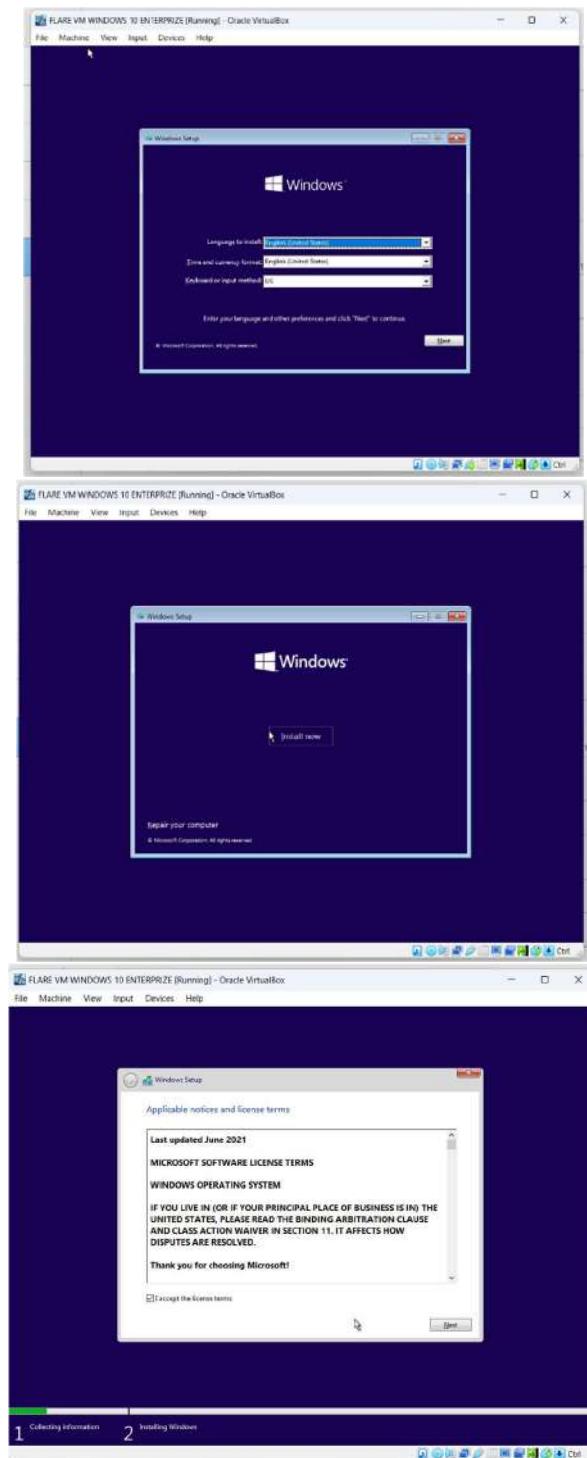
Leave the **Network Adapter** on its default setting of **NAT**.

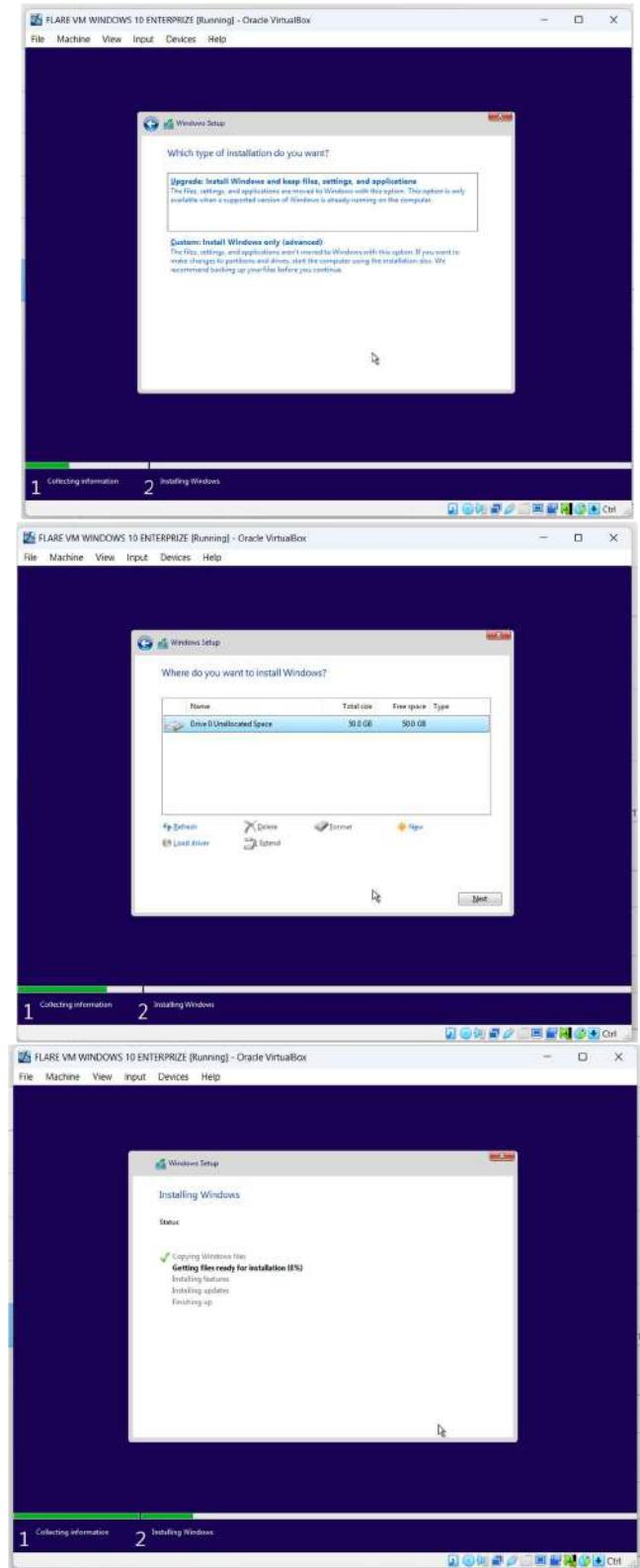


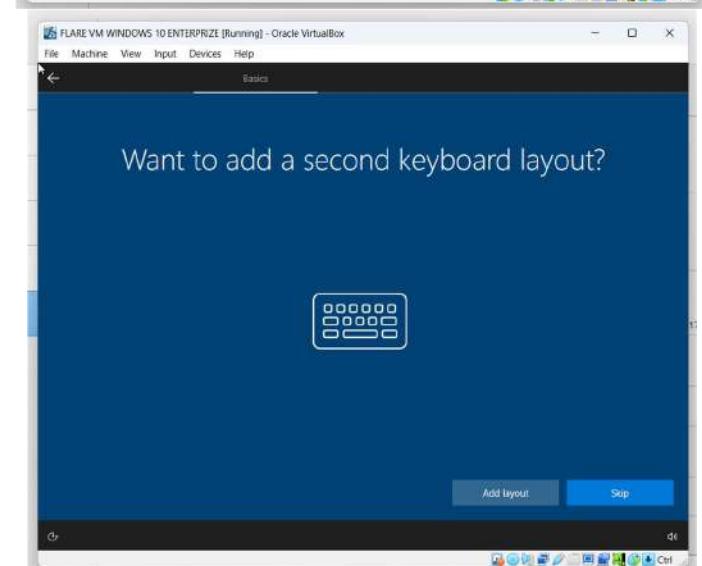
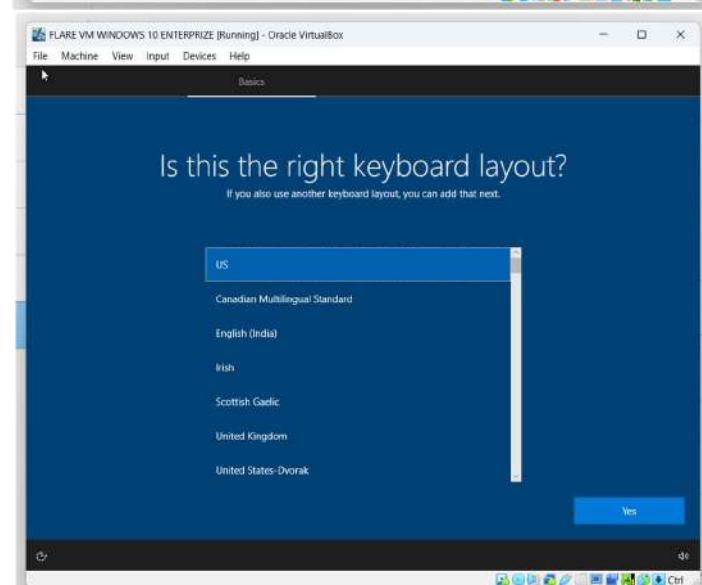
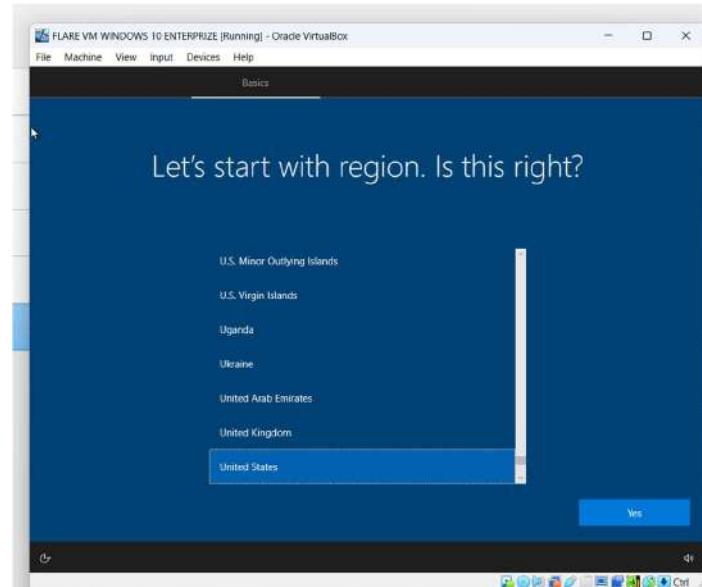
Click on **OK** to save the settings.

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

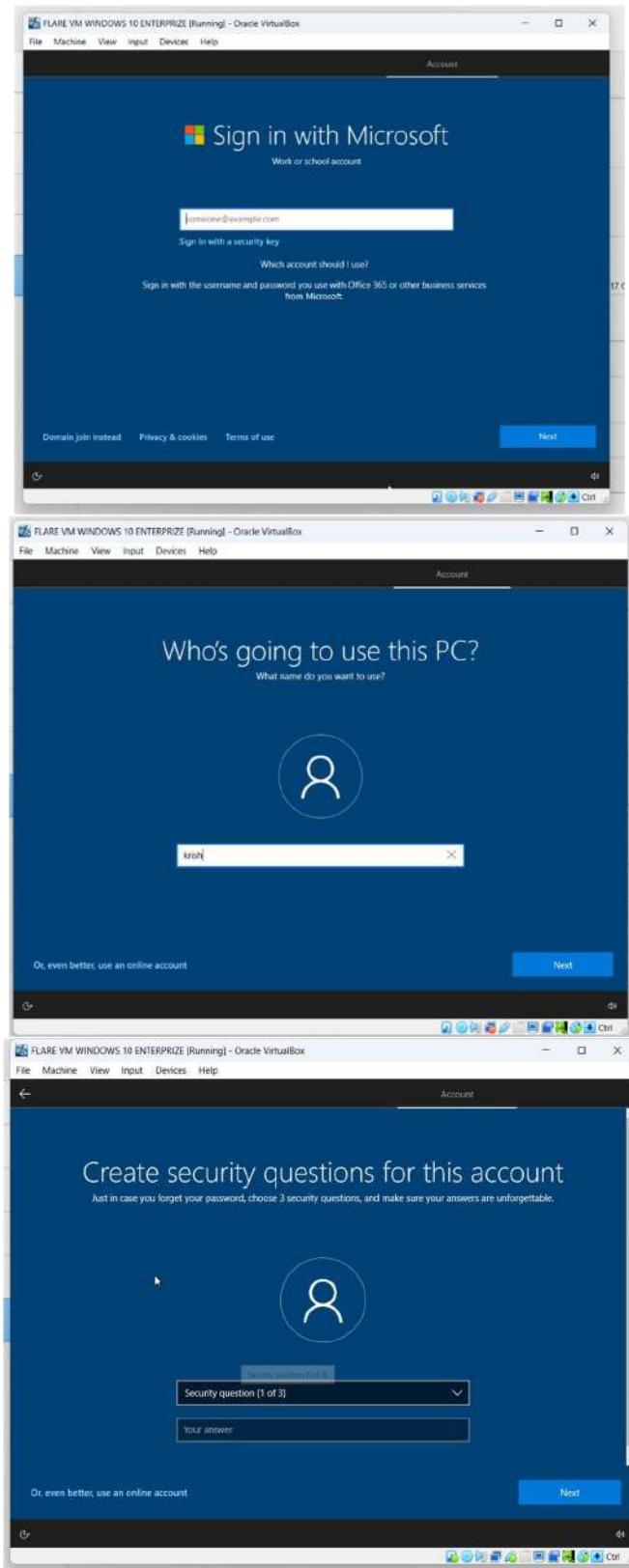
We can follow previous methods for installation.

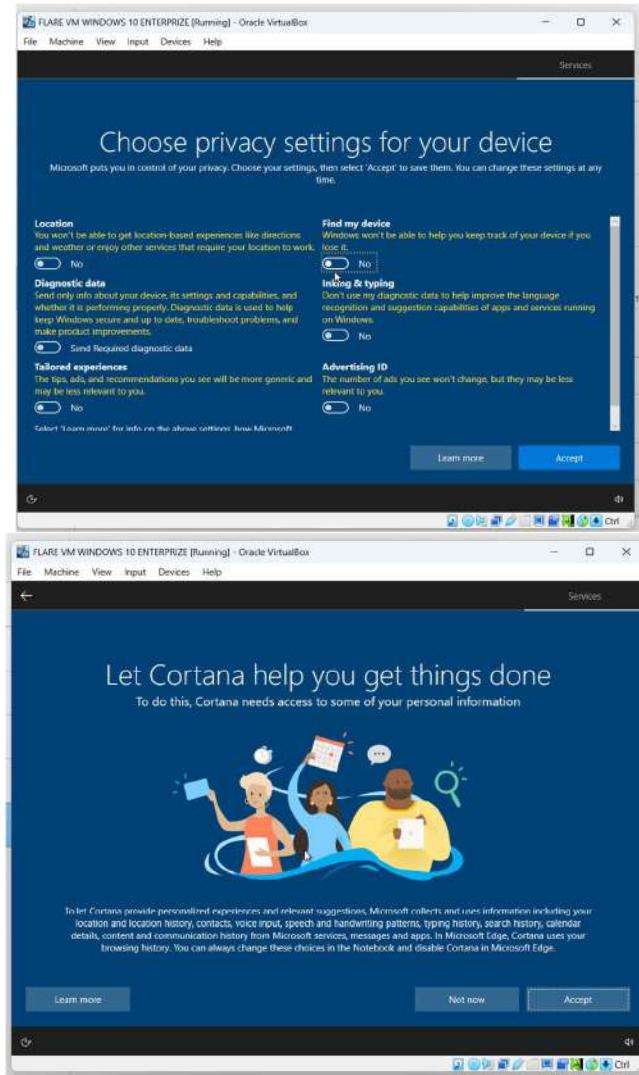




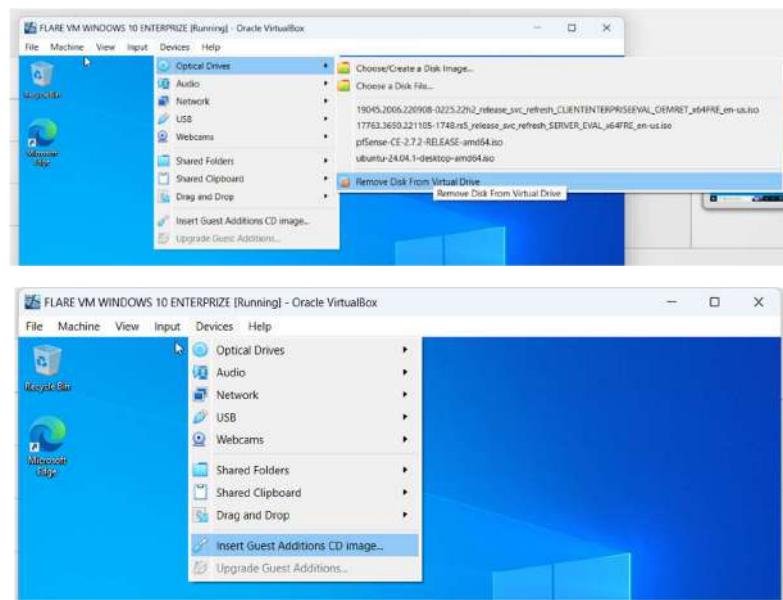


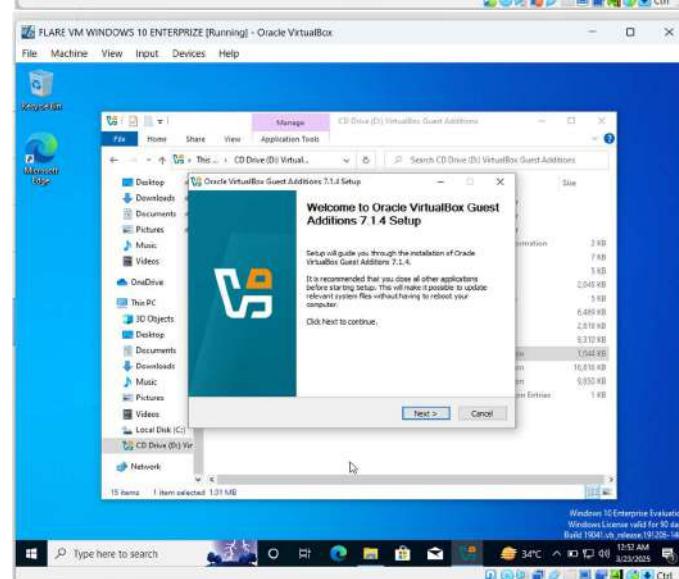
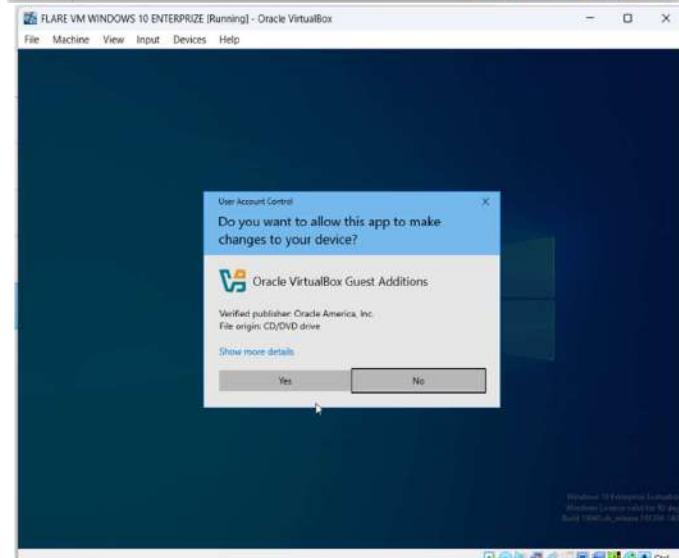
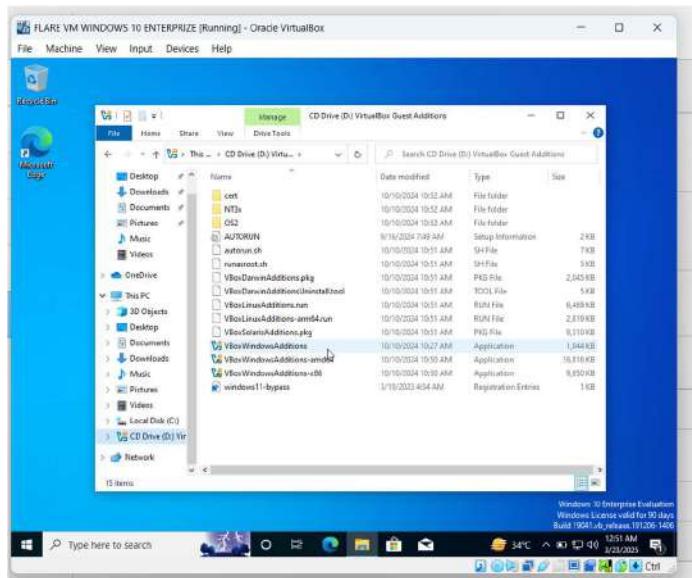
Select “Domain join instead”.

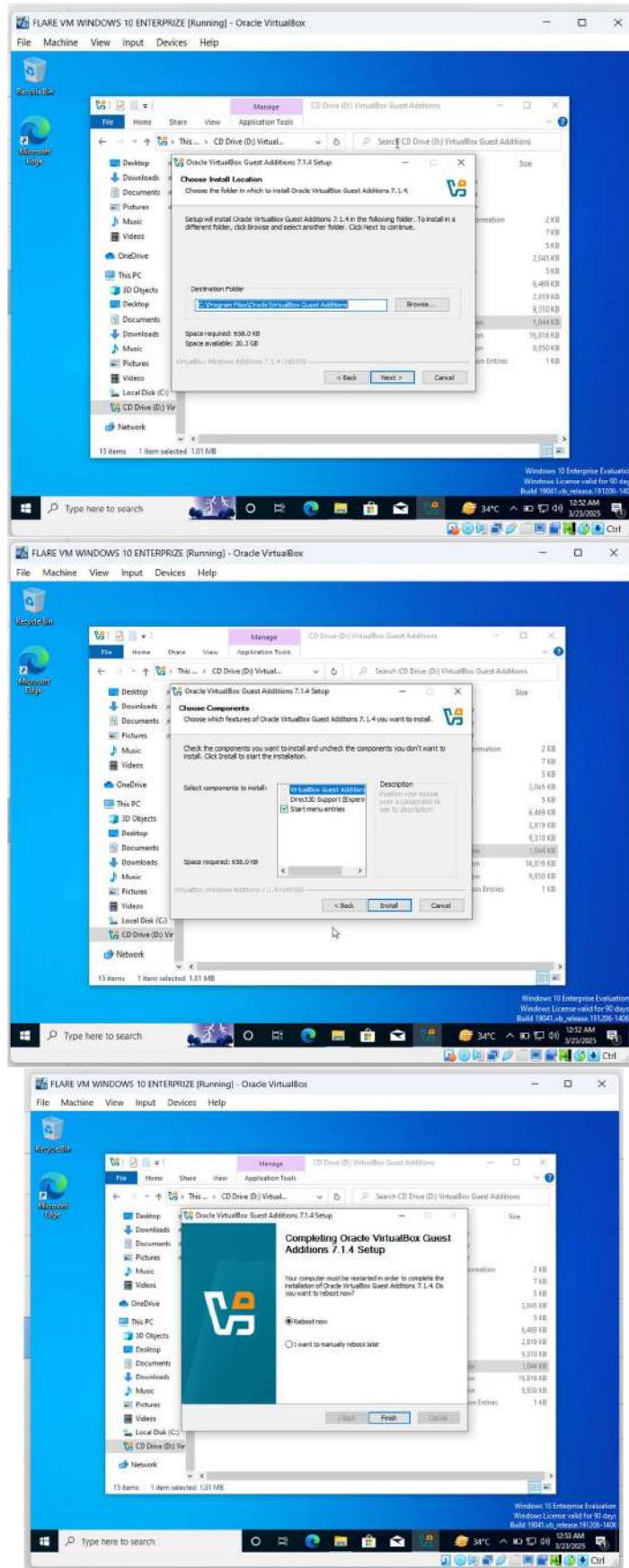




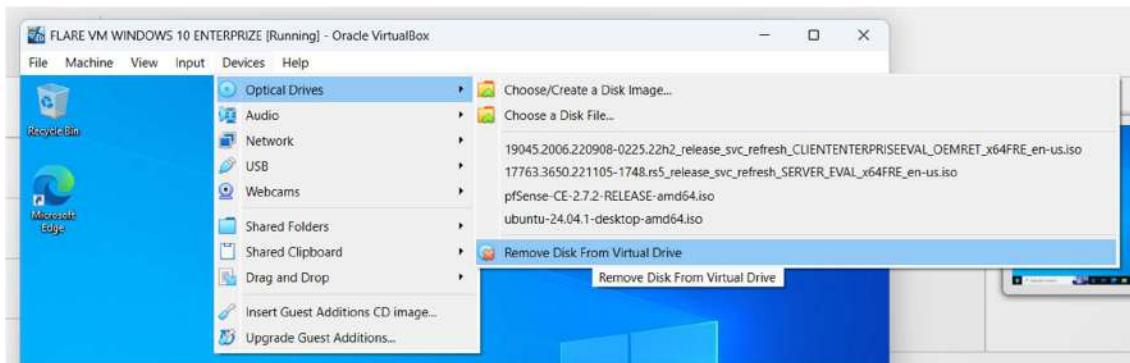
Install Guest Additions to enable the resizing on the VM display.





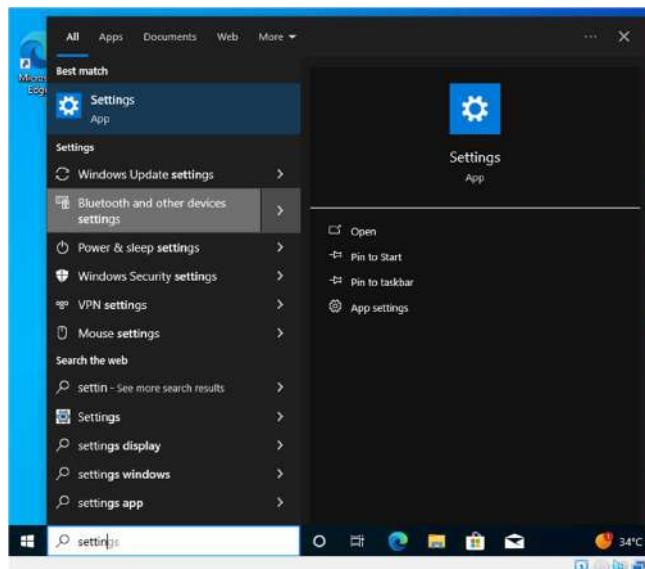


After rebooting the VM. Remove the Guest Addition Image.

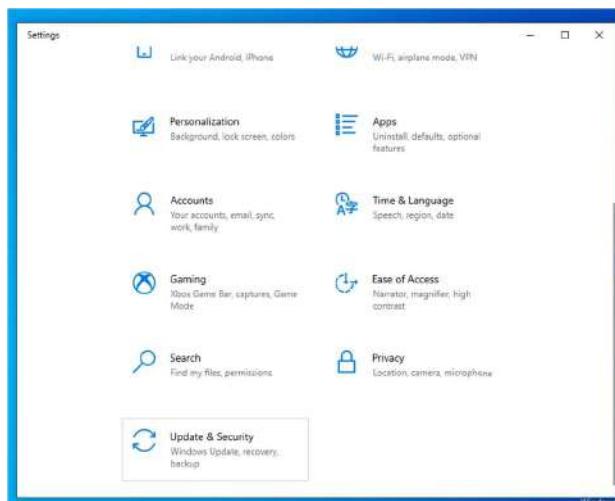


## Disabling Windows Update

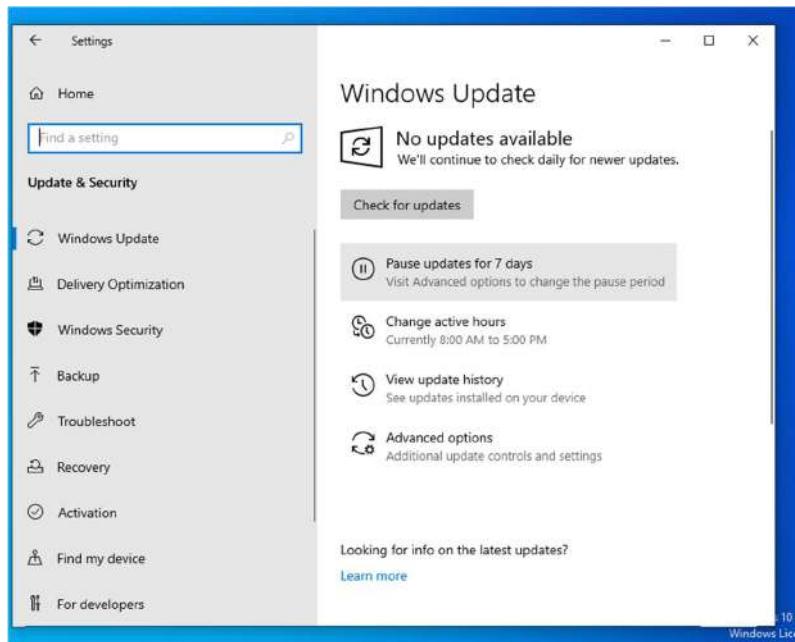
Open on Search bar and search for “Settings”. Open the Settings app.



Click on “Update & Security”



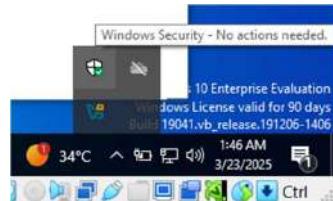
Click on the “Pause updates for 7 days” button.



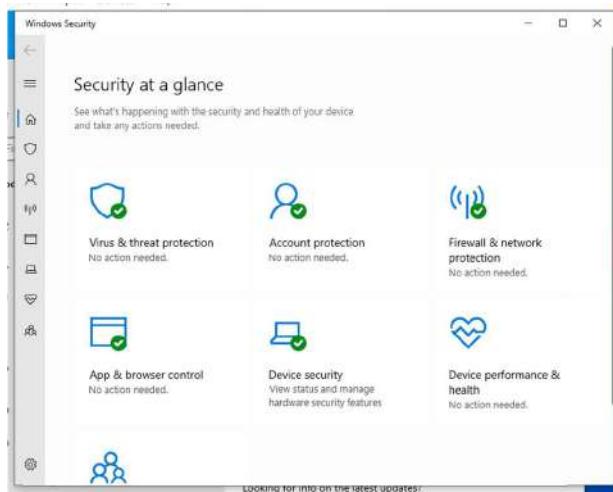
### Disabling Windows Defender

Download the following script: [jeremybeaume/tools: Script to disable Windows Defender](https://jeremybeaume/tools/)

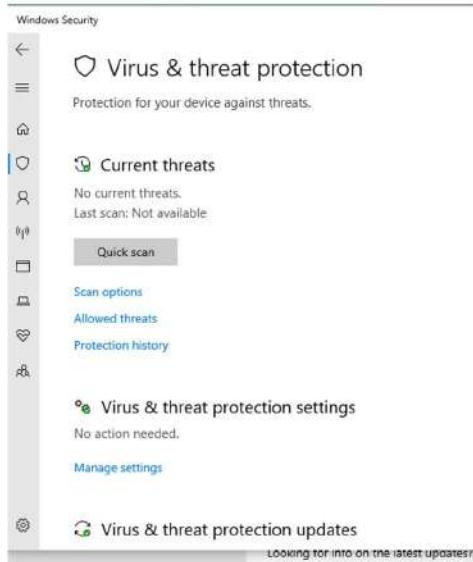
Right-click on the Shield icon on the taskbar and select “View Security Dashboard”.



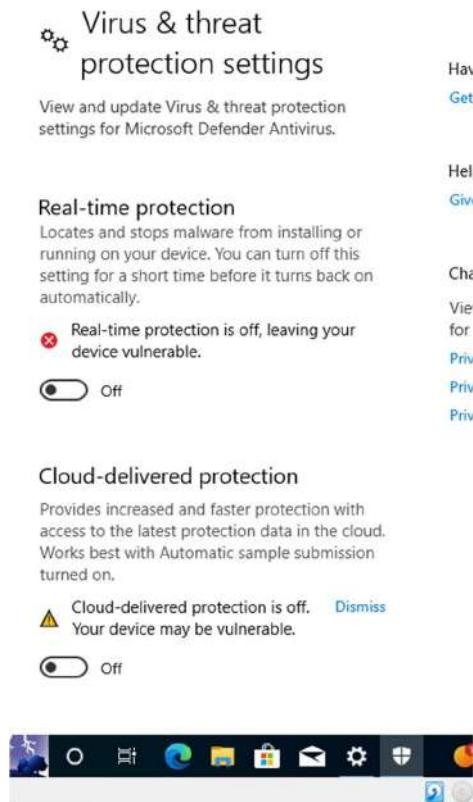
Click on “Virus & threat protection”.



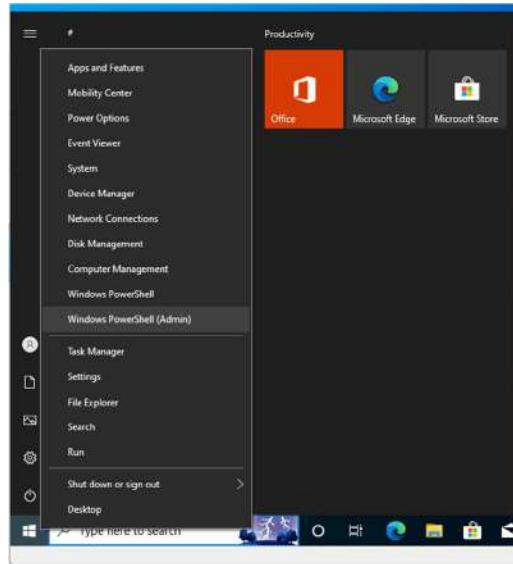
Select “Manage settings” from the “Virus & threat protection settings” section.



Disable all the features that are enabled:



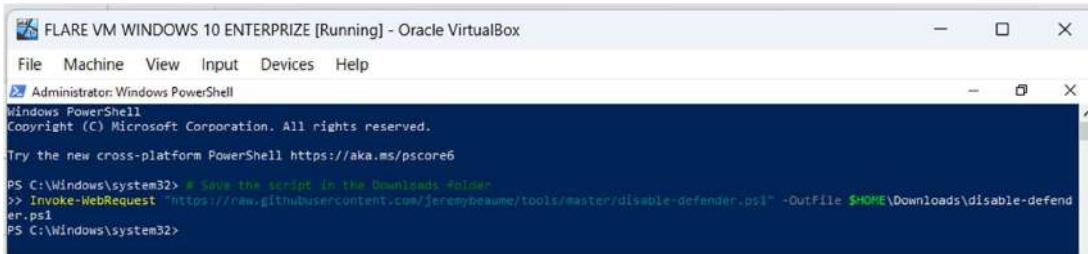
Right-click on the Start menu and select “Windows PowerShell (Admin)”.



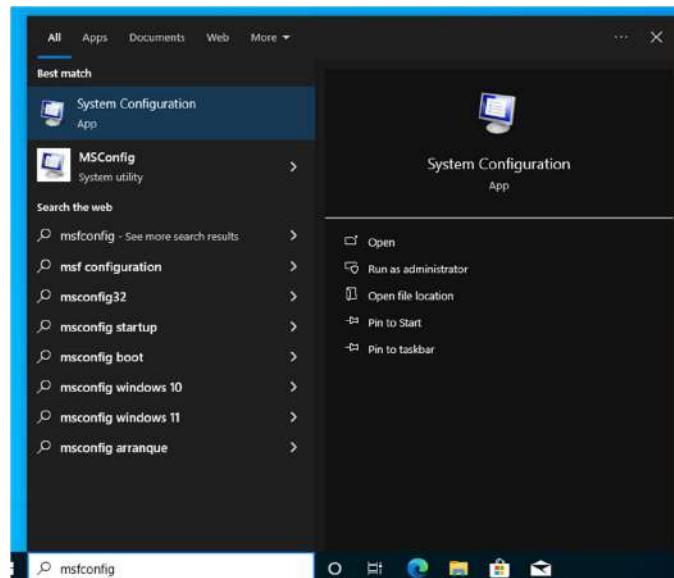
Run the following command to download the script:

```
# Save the script in the Downloads folder #
```

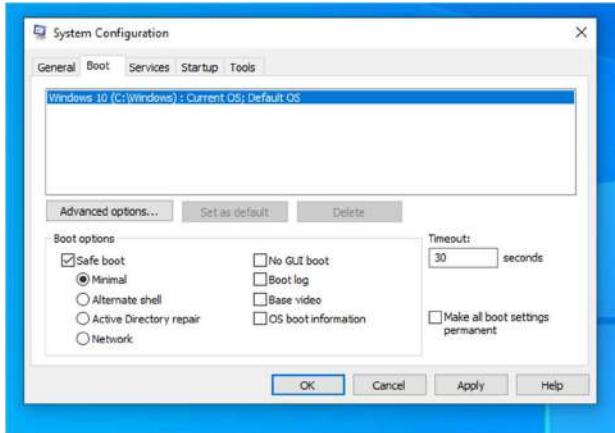
```
Invoke-WebRequest "https://raw.githubusercontent.com/jeremybeaume/tools/master/disable-defender.ps1" -OutFile $HOME\Downloads\disable-defender.ps1
```



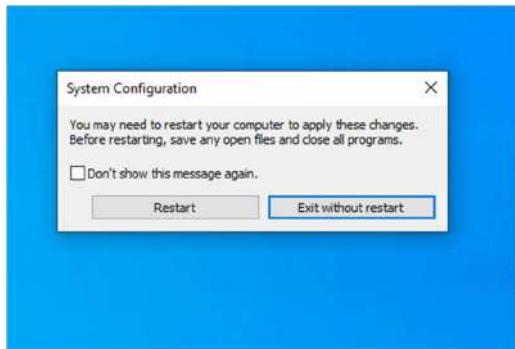
Search msfconfig then open.



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.



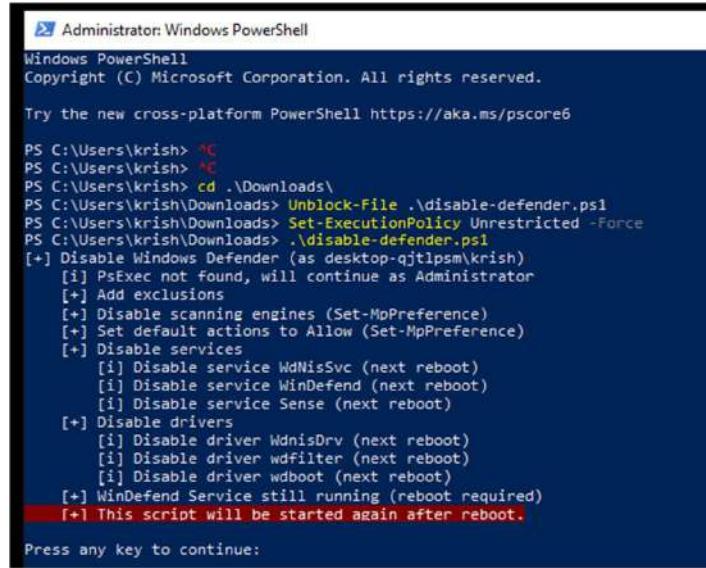
In Safe Mode, the VM cannot be resizable. Safe Mode essentially disables all features that are not required to run the OS.

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
```

```
PS C:\Users\krish> ^C  
PS C:\Users\krish> ^C  
PS C:\Users\krish> cd .\Downloads\  
PS C:\Users\krish\Downloads> Unblock-File .\disable-defender.ps1  
PS C:\Users\krish\Downloads> Set-ExecutionPolicy Unrestricted -Force  
PS C:\Users\krish\Downloads> .\disable-defender.ps1
```

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



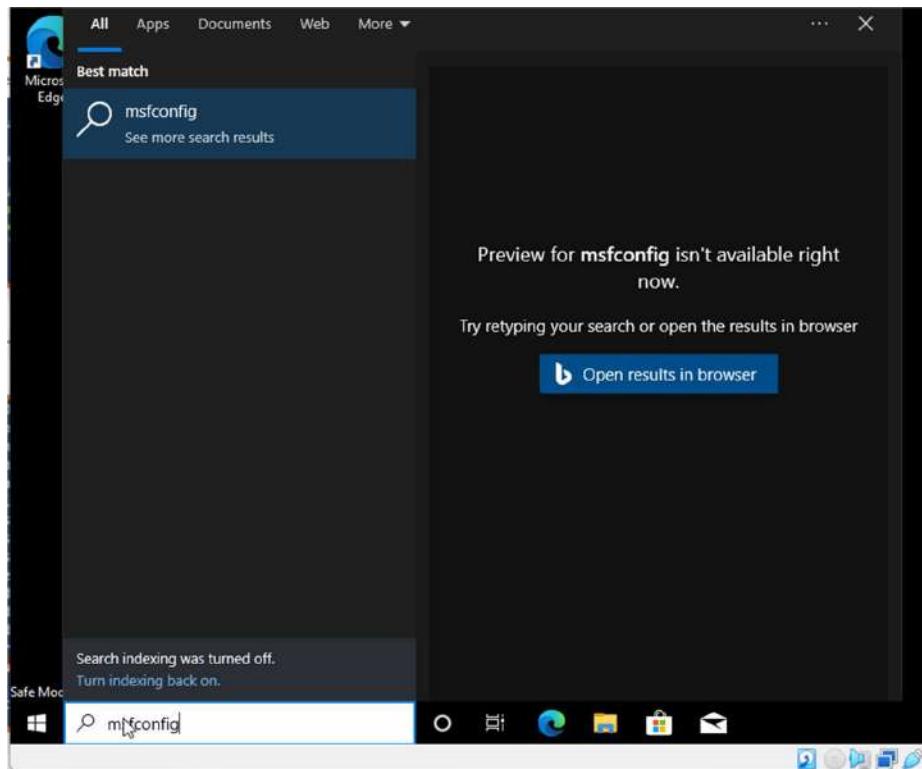
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

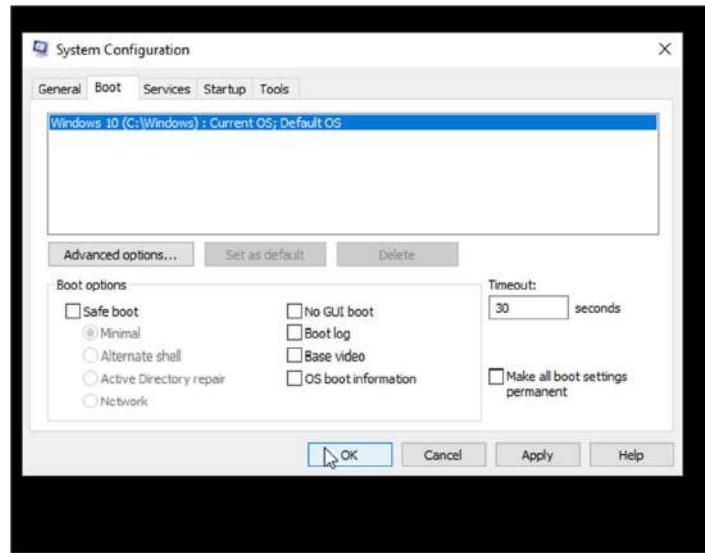
PS C:\Users\krish> <C>
PS C:\Users\krish> <C>
PS C:\Users\krish> cd .\Downloads\
PS C:\Users\krish\Downloads> Unblock-File .\disable-defender.ps1
PS C:\Users\krish\Downloads> Set-ExecutionPolicy Unrestricted -Force
PS C:\Users\krish\Downloads> .\disable-defender.ps1
[+] Disable Windows Defender (as desktop-qjtlpsm\krish)
  [i] PsExec not found, will continue as Administrator
  [+] Add exclusions
  [+] Disable scanning engines (Set-MpPreference)
  [+] Set default actions to Allow (Set-MpPreference)
  [+] Disable services
    [i] Disable service WdNisSvc (next reboot)
    [i] Disable service WinDefend (next reboot)
    [i] Disable service Sense (next reboot)
  [+] Disable drivers
    [i] Disable driver WdnisDrv (next reboot)
    [i] Disable driver wdfilter (next reboot)
    [i] Disable driver wdboot (next reboot)
  [+] WinDefend Service still running (reboot required)
  [+] This script will be started again after reboot.

Press any key to continue:
```

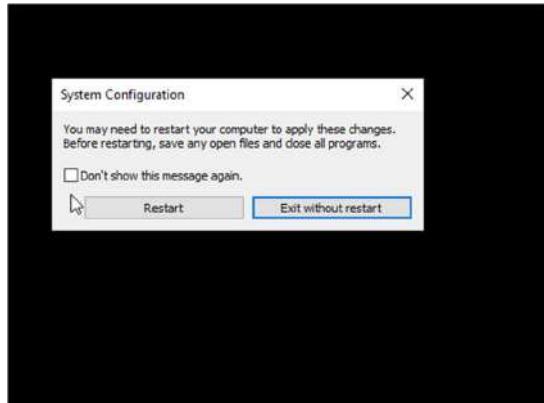
Click on search msconfig and open.



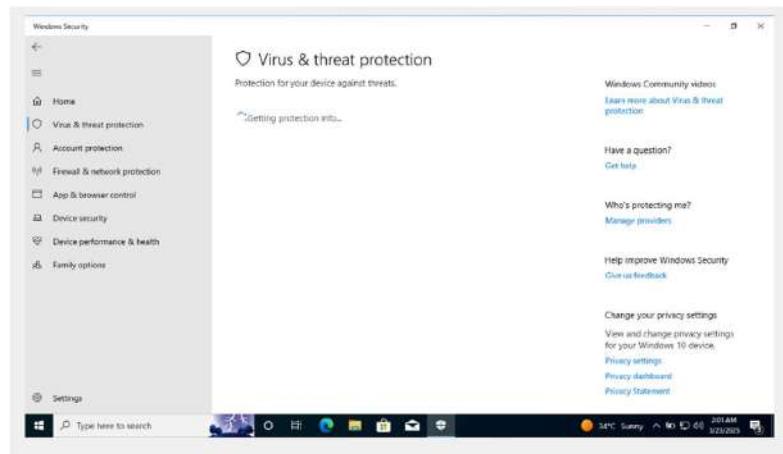
From the Boot options section disable “Safe boot”. Click on **Apply** then **OK**.



Then restart computer

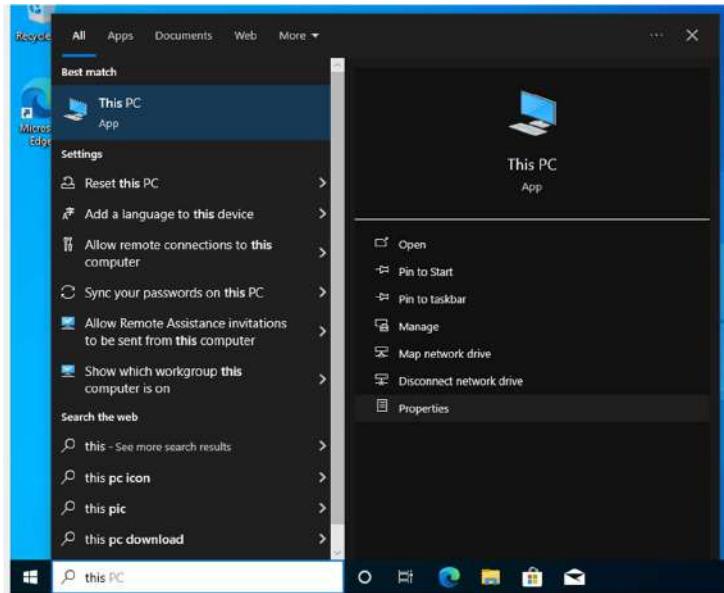


Wait for some time for Defender to load completely and then you will see that "Virus & threat protection" will show as disabled. This means that the script worked successfully.

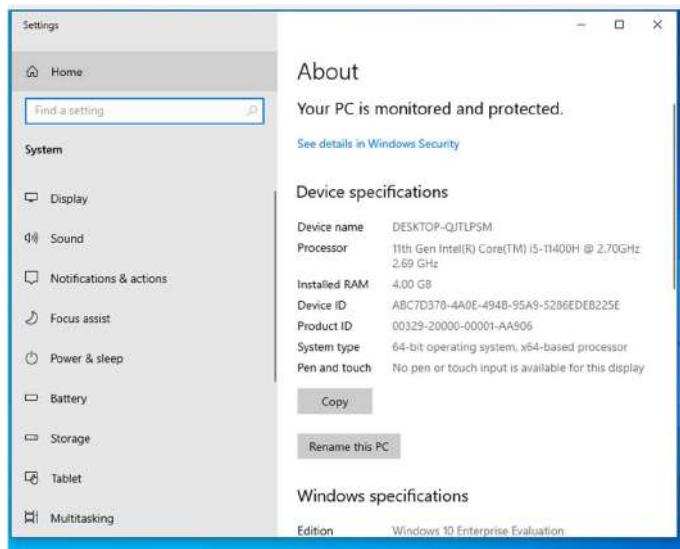


Renaming the VM

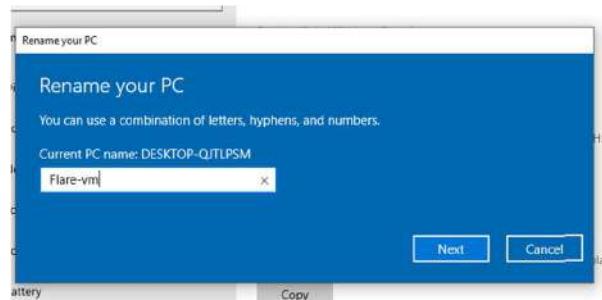
Search for "This PC" and from the right side click on "Properties".



Select "Rename this PC".

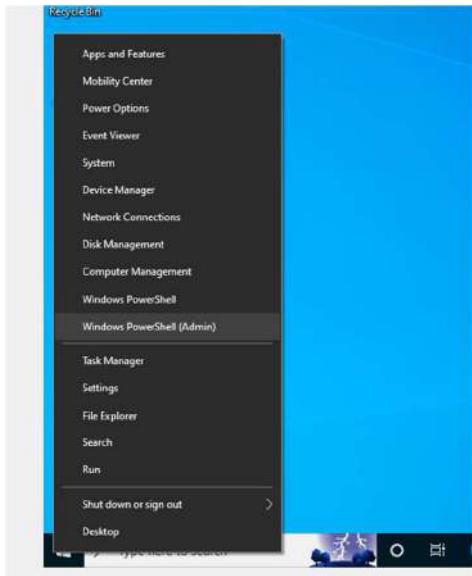


Give the PC a name. Click on **Next** and then select "Restart Now" for the changes to take effect.



## 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
```

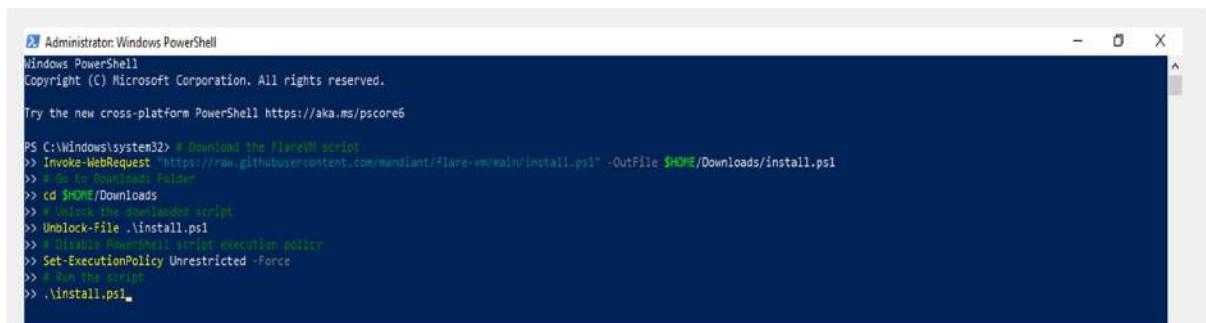
```
Unblock-File .\install.ps1
```

```
# Disable PowerShell script execution policy
```

```
Set-ExecutionPolicy Unrestricted -Force
```

```
# Run the script
```

```
.\install.ps1
```

A screenshot of an 'Administrator: Windows PowerShell' window. The window title is 'Administrator: Windows PowerShell'. The content shows a series of PowerShell commands being run in the terminal. The commands are:

```
PS C:\Windows\system32> # 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 downloaded script  
>> Unblock-File .\install.ps1  
>> # Disable PowerShell script execution policy  
>> Set-ExecutionPolicy Unrestricted -Force  
>> # Run the script  
>> .\install.ps1
```

The window has a dark blue background and a light blue header bar.

The script will make some checks before starting the installation.

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

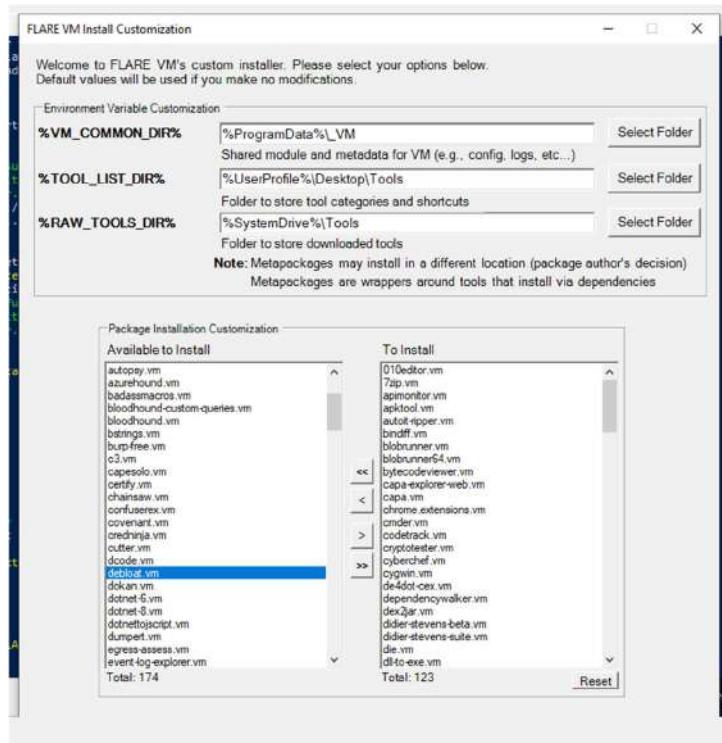
```
[-] Do you still wish to proceed? (Y/N): y
[+] Checking for Internet connectivity (google.com)...
[+] Internet connectivity check for google.com passed
[+] Checking for Internet connectivity (github.com)...
[+] Internet connectivity check for github.com passed
[+] Checking for Internet connectivity (raw.githubusercontent.com)...
[+] Internet connectivity check for raw.githubusercontent.com passed
[+] Network connectivity looks good
[+] Checking if Windows Defender Tamper Protection is disabled...
[+] Tamper Protection is disabled
[+] Checking if Windows Defender service is disabled...
[+] Defender is disabled
[+] Setting password to never expire to avoid that a password expiration blocks the installation...
[-] Have you taken a VM snapshot to ensure you can revert to pre-installation state? (Y/N): y
[+] Getting user credentials ...

Windows PowerShell credential request
Enter your credentials.
Password for user krish: *****
```

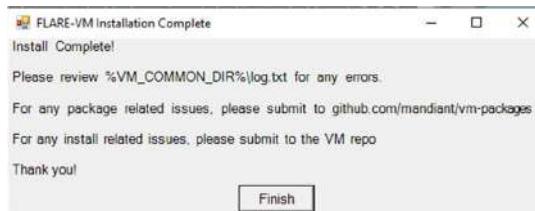
After some time the Flare VM configuration dialog will open.

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

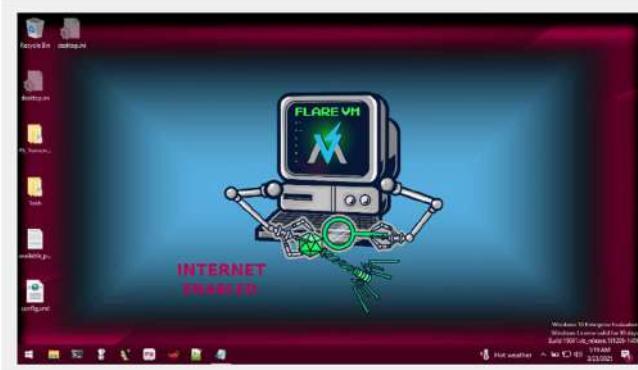
Click on **OK** to start the install. The VM will restart multiple times during the setup



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.

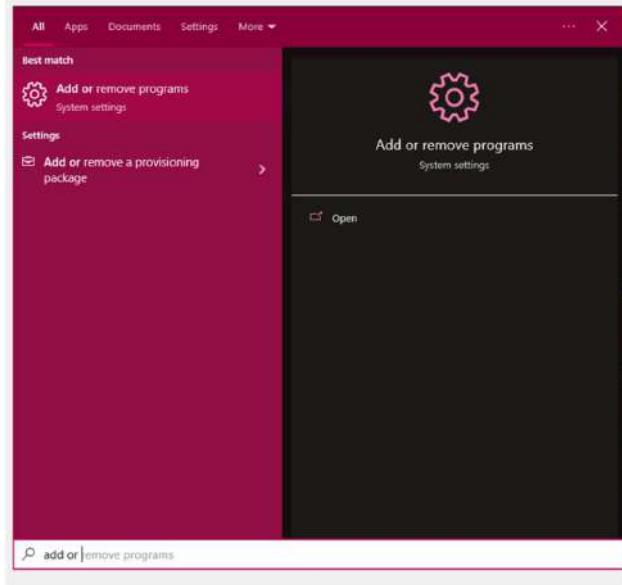


### Post-Install Configuration

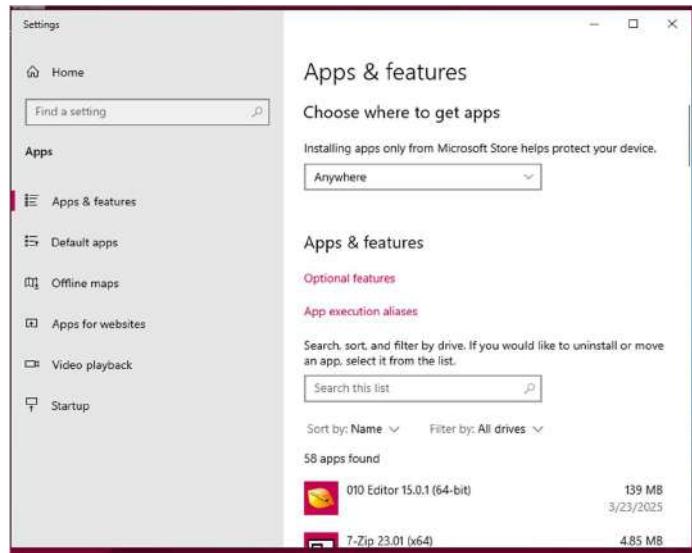
#### Installing OpenSSH Server

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](#)".

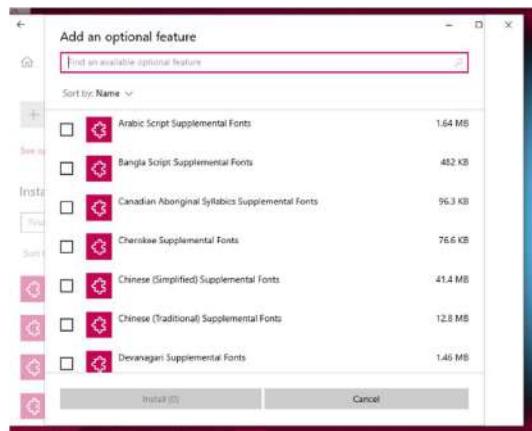
Open the Search bar. Type "Add" and from the results select the "[Add or remove programs](#)" option.



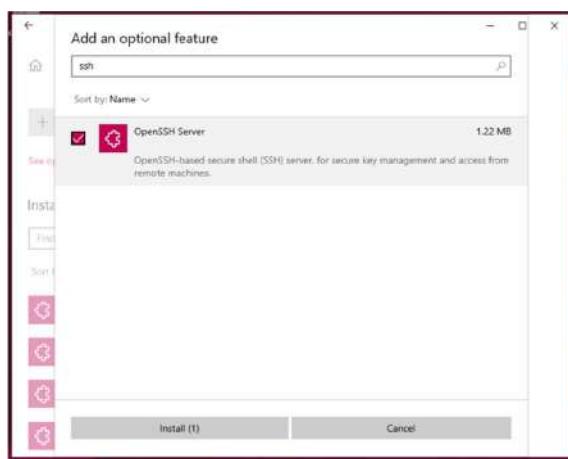
Click on **Optional Features** under "[Apps & features](#)".



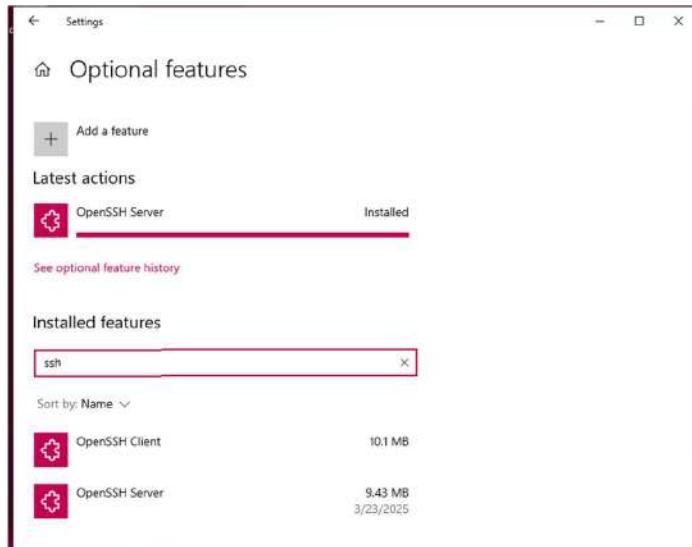
Click on **Add a feature**. This will open a new menu.



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

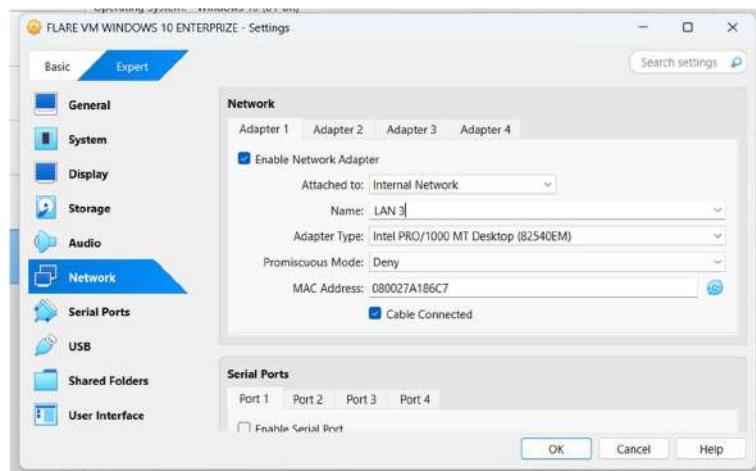


Once the install is complete if you search for “SSH” in the “Installed features” section you should see “OpenSSH Client” and “OpenSSH Server”.



## 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
```

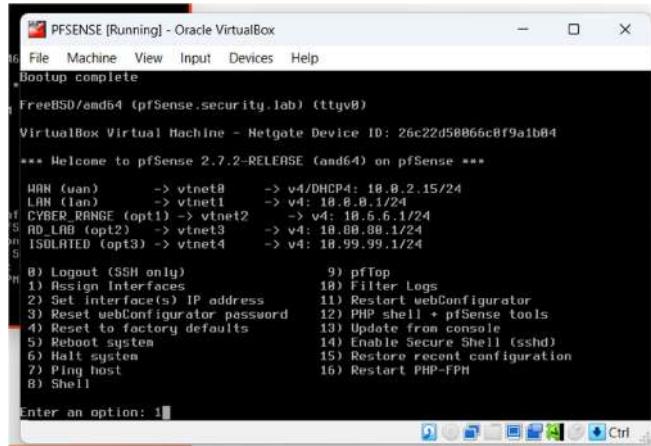
```
VBoxManage modifyvm "PFSENSE" --cableconnected6 on
```

```
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**

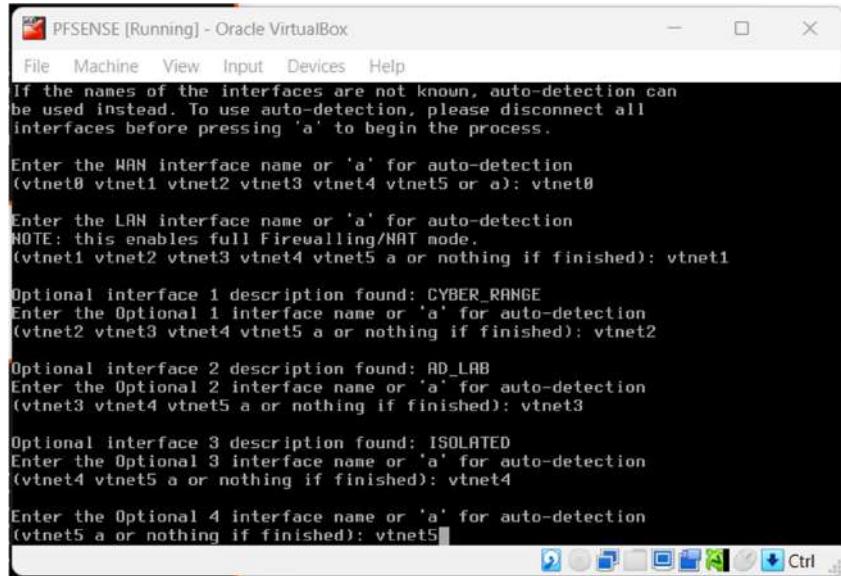
Enter the LAN interface name: **vtnet1**

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**



```

PFSense [Running] - Oracle VirtualBox
File Machine View Input Devices Help
If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(vtнет0 vtнет1 vtнет2 vtнет3 vtнет4 vtнет5 or a): vtнет0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(vtнет1 vtнет2 vtнет3 vtнет4 vtнет5 a or nothing if finished): vtнет1

Optional interface 1 description found: CYBER_RANGE
Enter the Optional 1 interface name or 'a' for auto-detection
(vtнет2 vtнет3 vtнет4 vtнет5 a or nothing if finished): vtнет2

Optional interface 2 description found: AD_LAB
Enter the Optional 2 interface name or 'a' for auto-detection
(vtнет3 vtнет4 vtнет5 a or nothing if finished): vtнет3

Optional interface 3 description found: ISOLATED
Enter the Optional 3 interface name or 'a' for auto-detection
(vtнет4 vtнет5 a or nothing if finished): vtнет4

Enter the Optional 4 interface name or 'a' for auto-detection
(vtнет5 a or nothing if finished): vtнет5

```

Do you want to proceed?: y



```

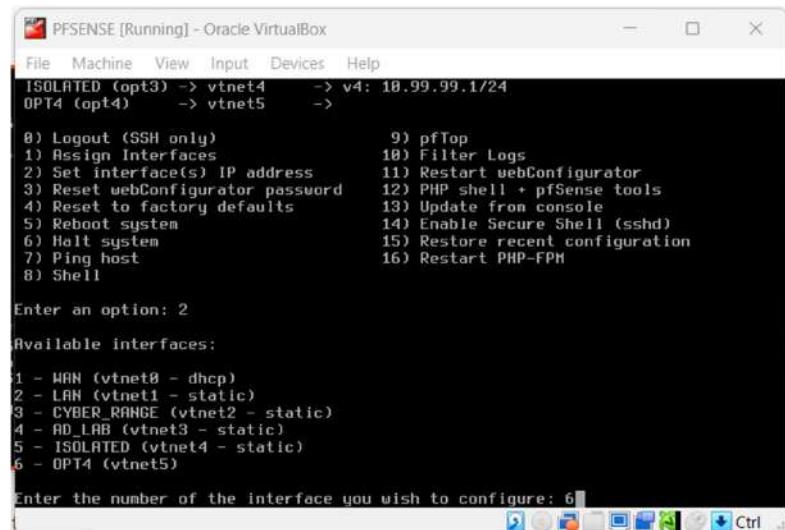
The interfaces will be assigned as follows:
WAN -> vtнет0
LAN -> vtнет1
OPT1 -> vtнет2
OPT2 -> vtнет3
OPT3 -> vtнет4
OPT4 -> vtнет5

Do you want to proceed [y/n]? 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.



```

File Machine View Input Devices Help
ISOLATED (opt3) -> vtнет4 -> v4: 10.99.99.1/24
OPT4 (opt4) -> vtнет5 ->

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

Enter an option: 2

Available interfaces:
1 - WAN (vtнет0 - dhcp)
2 - LAN (vtнет1 - static)
3 - CYBER_RANGE (vtнет2 - static)
4 - AD_LAB (vtнет3 - static)
5 - ISOLATED (vtнет4 - static)
6 - OPT4 (vtнет5)

Enter the number of the interface you wish to configure: 6

```

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**

```
3 - CYBER RANGE (vtnet2 - static)
4 - RD_LAB (vtnet3 - static)
5 - ISOLATED (vtnet4 - static)
6 - OPT4 (vtnet5)

Enter the number of the interface you wish to configure: 6
Configure IPv4 address OPT4 interface via DHCP? (y/n) n
Enter the new OPT4 IPv4 address. Press <ENTER> for none:
> 10.10.10.11

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0 = 16
      255.0.0.0 = 8

Enter the new OPT4 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT4 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT4 interface via DHCP6? (y/n) n

Configure IPv6 address OPT4 interface via DHCP6? (y/n) n
Enter the new OPT4 IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on OPT4? (y/n) 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
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Now interface OPT4 will have an IP address.

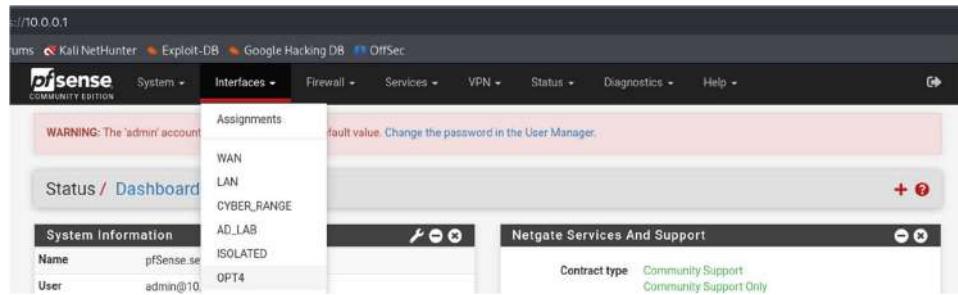
```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
HAN (wan)      -> vtnet0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet1      -> v4: 10.0.0.1/24
CYBER_RANGE (opt1) -> vtnet2      -> v4: 10.6.6.1/24
RD_LAB (opt2)  -> vtnet3      -> v4: 10.00.00.1/24
ISOLATED (opt3) -> vtnet4      -> v4: 10.99.99.1/24
OPT4 (opt4)    -> vtnet5      -> v4: 10.10.10.1/24

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

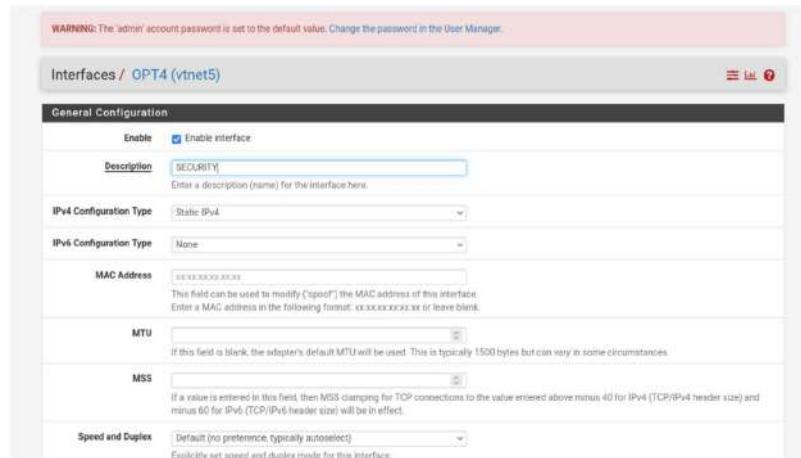
Enter an option: 1
```

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**.

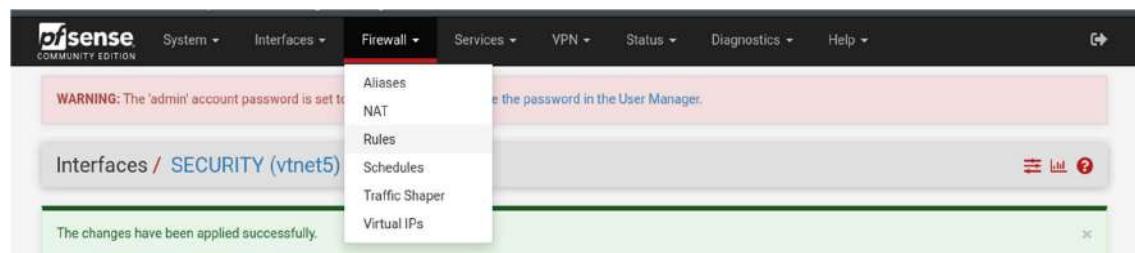


Click on **Apply Changes** in the popup that appears to persist the changes.



## 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.

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / SECURITY

Floating WAN LAN CYBER\_RANGE AD\_LAB ISOLATED SECURITY

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
No rules are currently defined for this interface All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.										

**Add** **Up** **Down** **Delete** **Toggle** **Copy** **Save** **Separator**

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**.

Action: Block

Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled:  Disable this rule  
Set this option to disable this rule without removing it from the list.

Interface: SECURITY

Address Family: IPv4+IPv6

Protocol: Any

Source

Source: SECURITY subnets

Destination

Destination: WAN subnets

Extra Options

Log:  Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: block access to services on wan interface

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**

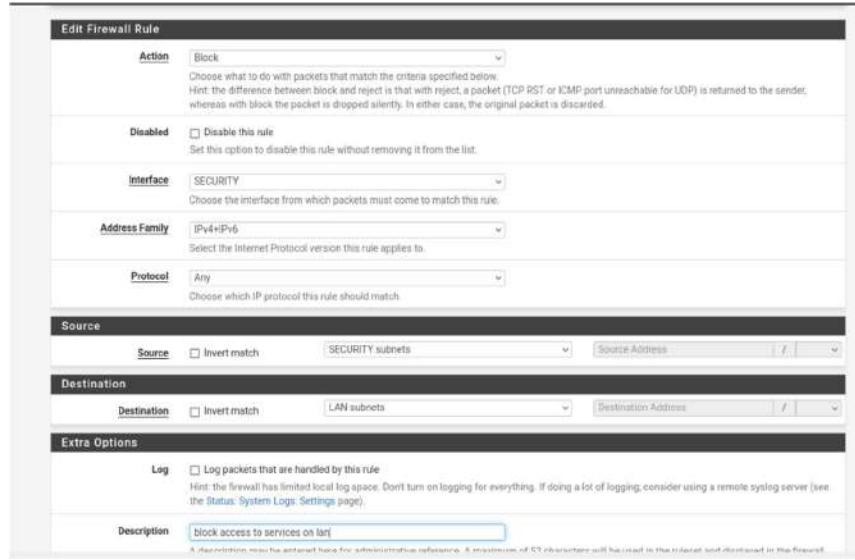
Protocol: **Any**

Source: **SECURITY subnets**

Destination: **LAN subnets**

Description: **Block access to services on LAN**

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



The screenshot shows the 'Edit Firewall Rule' dialog box. The 'Action' dropdown is set to 'Block'. The 'Disabled' checkbox is unchecked. The 'Interface' dropdown is set to 'SECURITY'. The 'Address Family' dropdown is set to 'IPv4+IPv6'. The 'Protocol' dropdown is set to 'Any'. The 'Source' section shows 'Source' set to 'Invert match' and 'SECURITY subnets' selected. The 'Destination' section shows 'Destination' set to 'Invert match' and 'LAN subnets' selected. The 'Extra Options' section has the 'Log' checkbox unchecked. The 'Description' field contains the text 'block access to services on lan'.

Click on “Add” to create a new rule.

Change the values as follows:

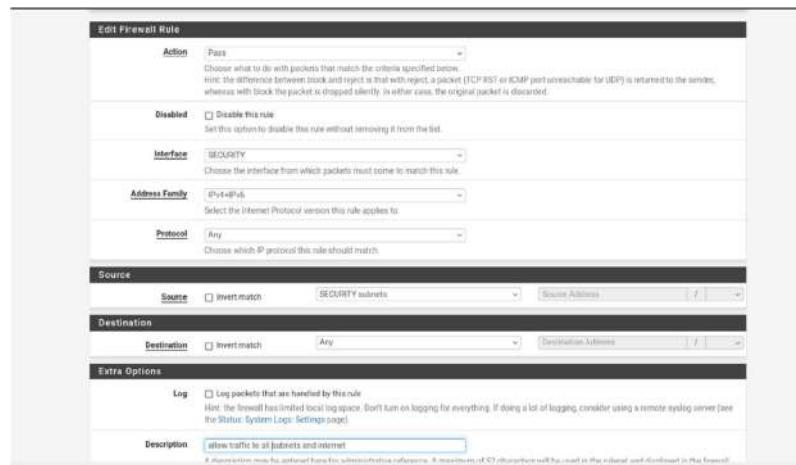
Address Family: **IPv4+IPv6**

Protocol: **Any**

Source: **SECURITY subnets**

Description: **Allow traffic to all subnets and Internet**

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



The screenshot shows the 'Edit Firewall Rule' dialog box. The 'Action' dropdown is set to 'Pass'. The 'Disabled' checkbox is unchecked. The 'Interface' dropdown is set to 'SECURITY'. The 'Address Family' dropdown is set to 'IPv4+IPv6'. The 'Protocol' dropdown is set to 'Any'. The 'Source' section shows 'Source' set to 'Invert match' and 'SECURITY subnets' selected. The 'Destination' section shows 'Destination' set to 'Invert match' and 'Any' selected. The 'Extra Options' section has the 'Log' checkbox unchecked. The 'Description' field contains the text 'allow traffic to all subnets and internet'.

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

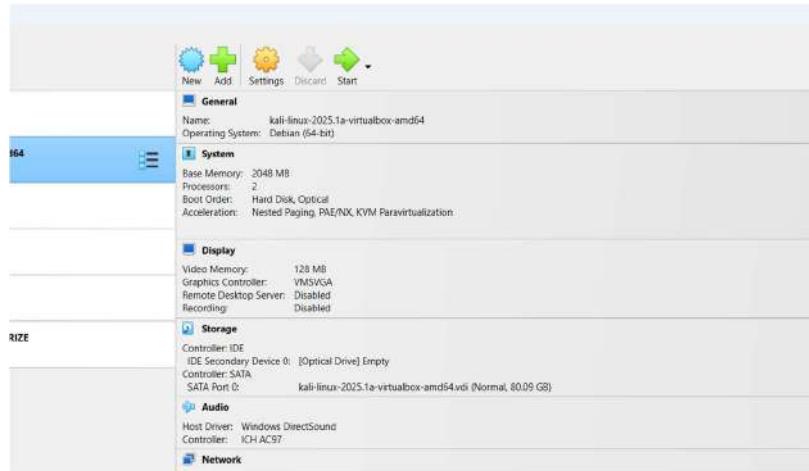
Go to the following URL: [Download Ubuntu Desktop | Download | Ubuntu](https://www.ubuntu.com/download/desktop).

Download the latest LTS version of Ubuntu. As of writing the latest version is **2022.04.3**

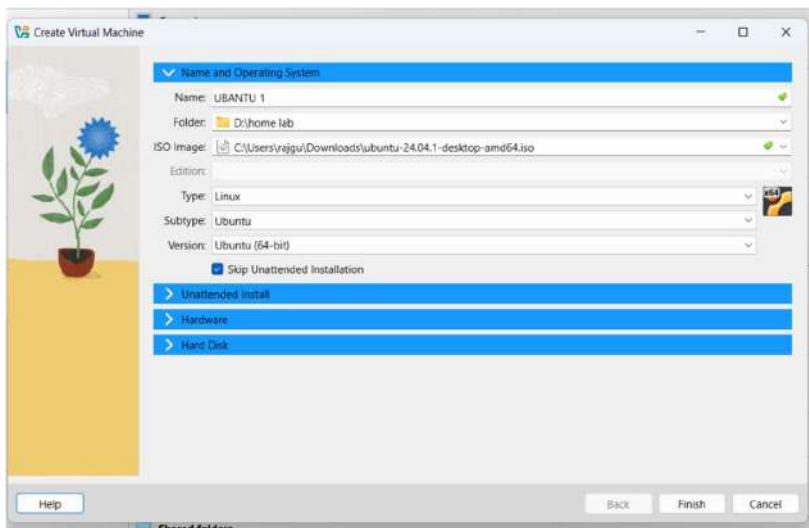
The ISO is ~5GB.

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

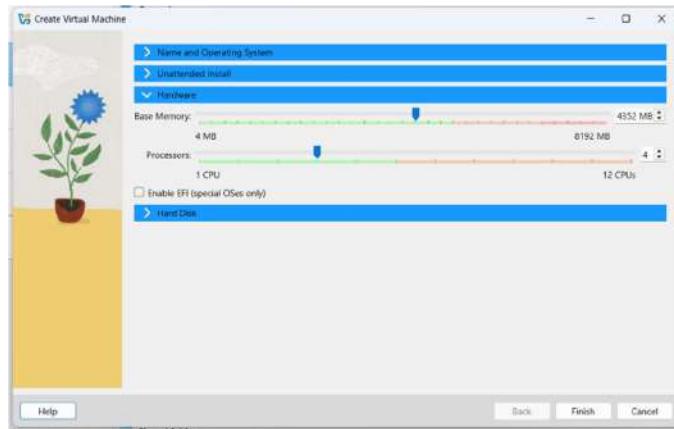
In VirtualBox from the sidebar select **Tools** and then click on **New** from the toolbar.



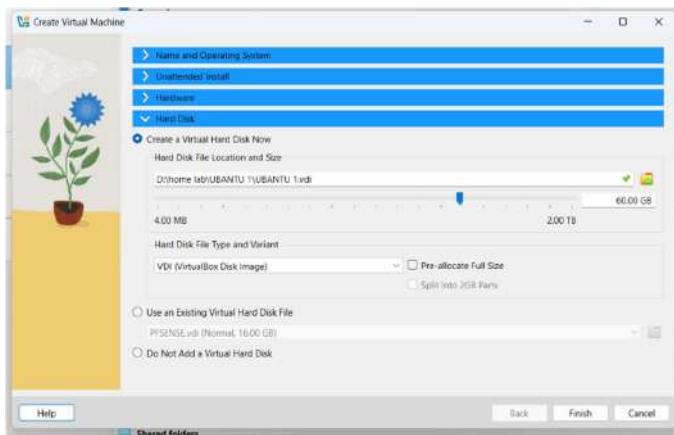
Give the VM a name. Select the downloaded ISO image. Select the “Skip Unattended Installation” option and click on **Next**.



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

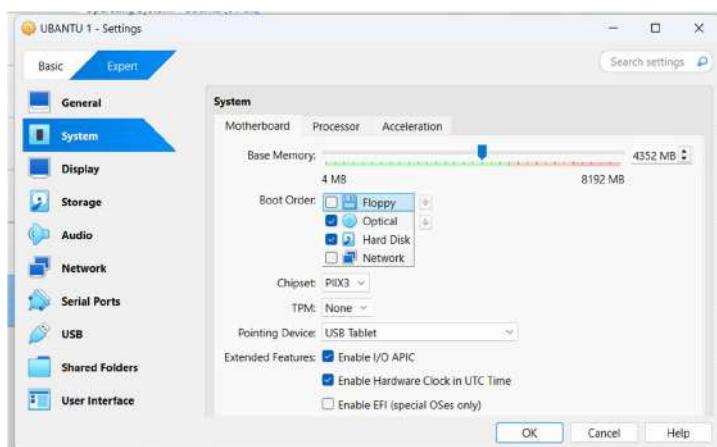


Increase the Hard Disk size to **60GB** and click on **Finish**.

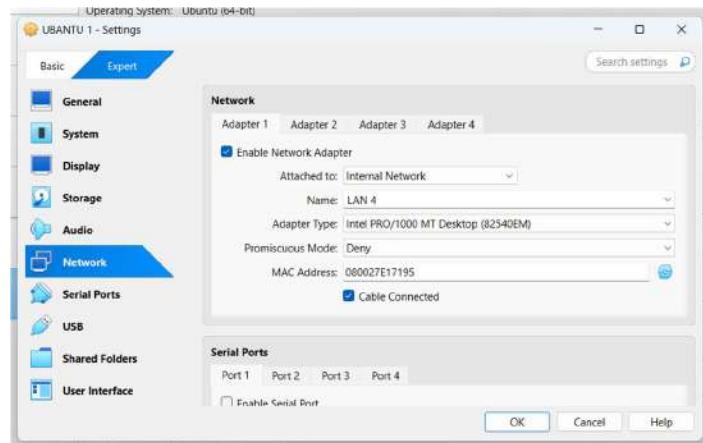


Select the VM and click on **Settings** from the toolbar.

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

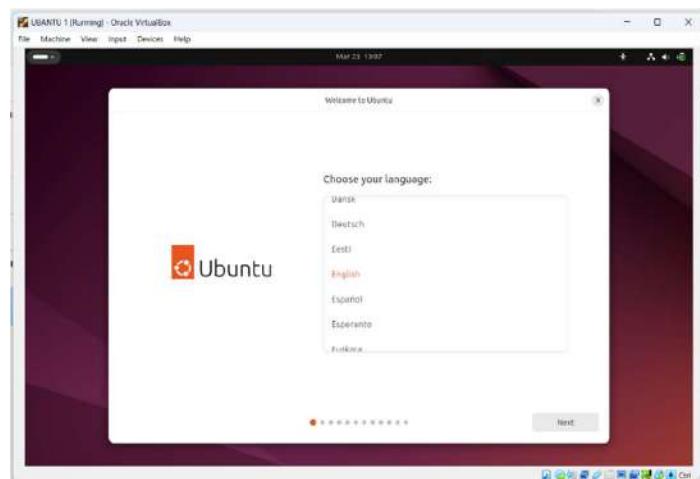


Go to **Network** -> **Adapter 1**. For the Attached to field select **Internal Network**. For name select **LAN 4**. Click on **OK** to save changes.

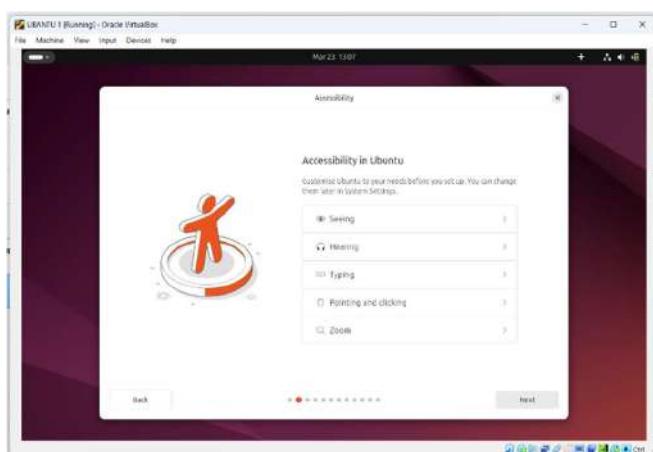


Select the VM and click on **Start**.

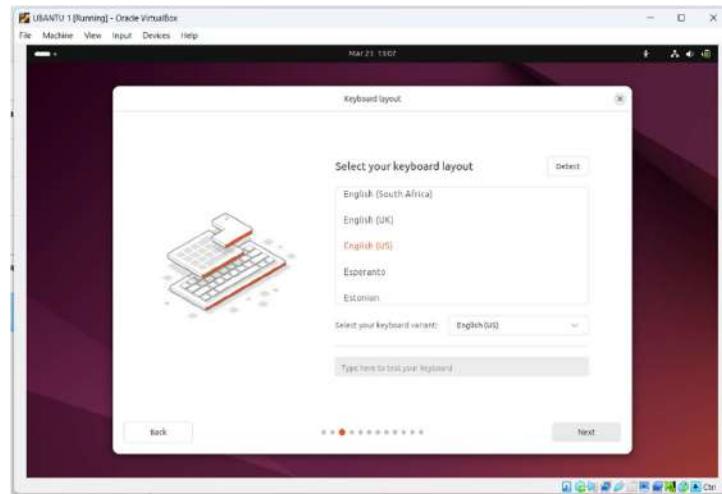
Then Click **Next**.



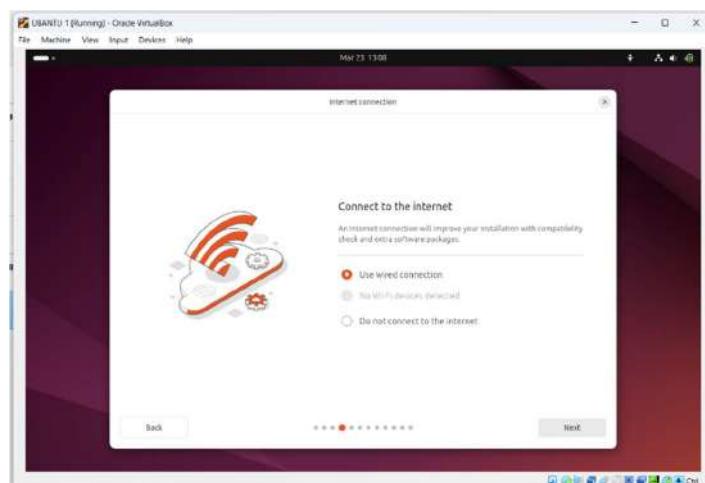
Then Click **Next**.



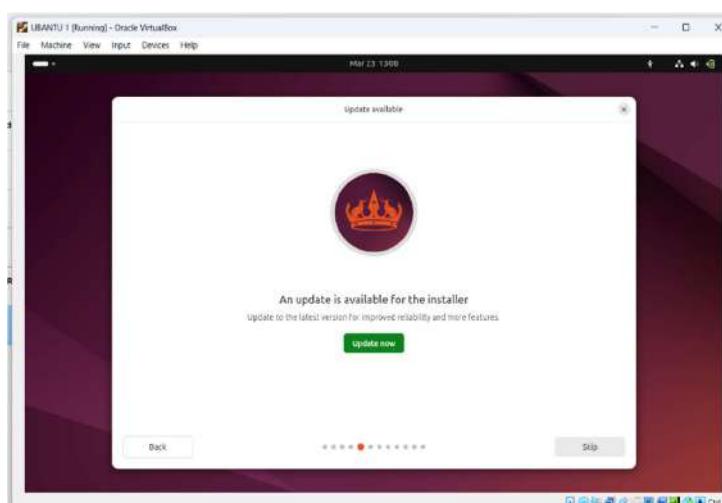
Then Click **Next**.



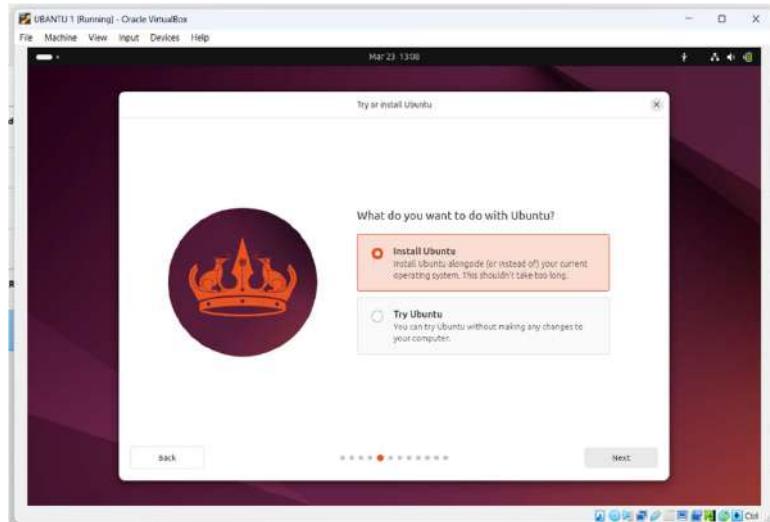
Then Click **Next**.



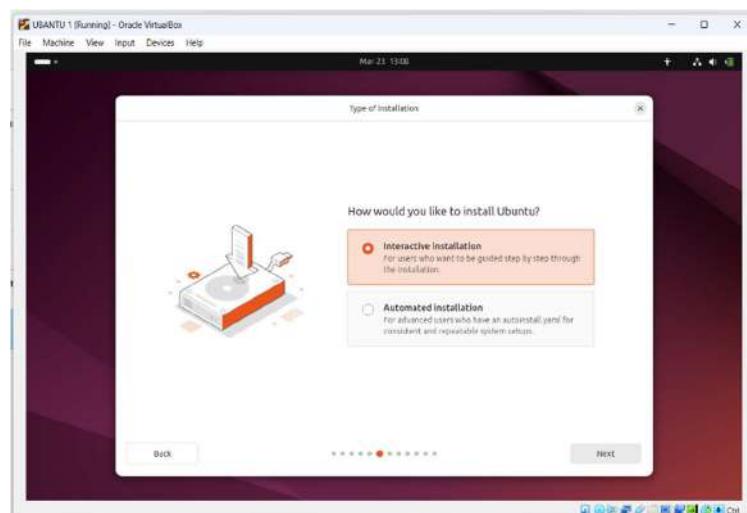
Then Click **Skip**.



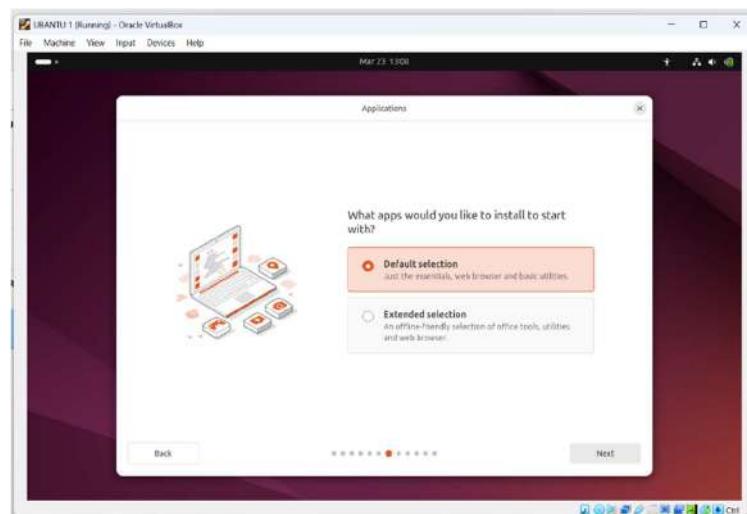
Then Click **Next**.



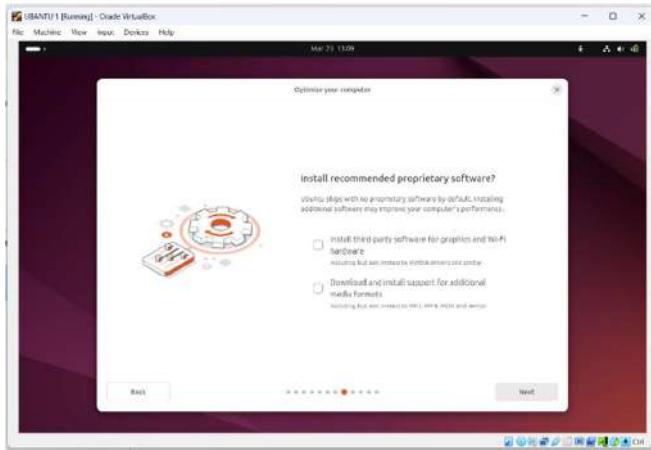
Then Click **Next**.



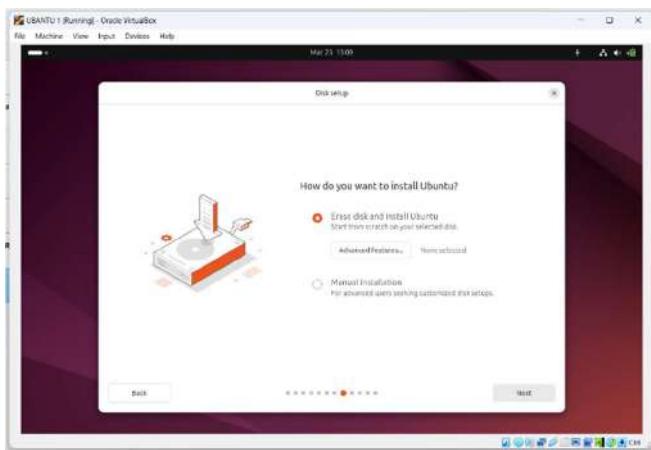
Then Click **Next**.



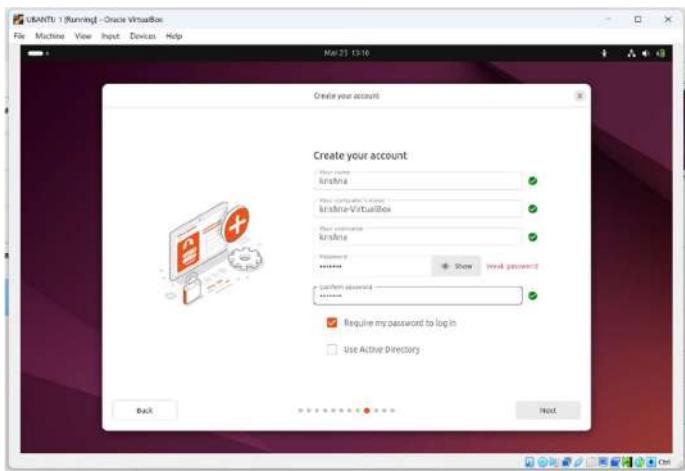
Then Click **Next**.



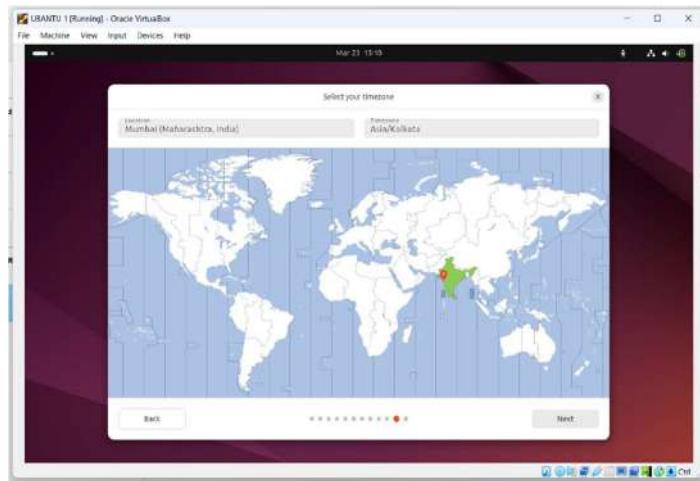
Then Click **Next**.



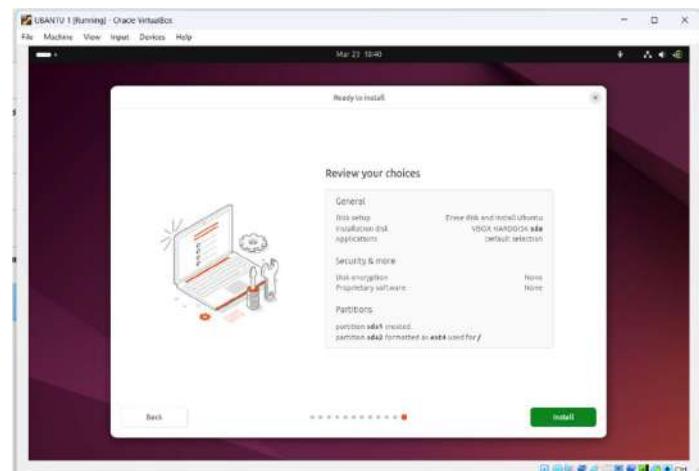
Enter the username, password and hostname and click on **Next**.



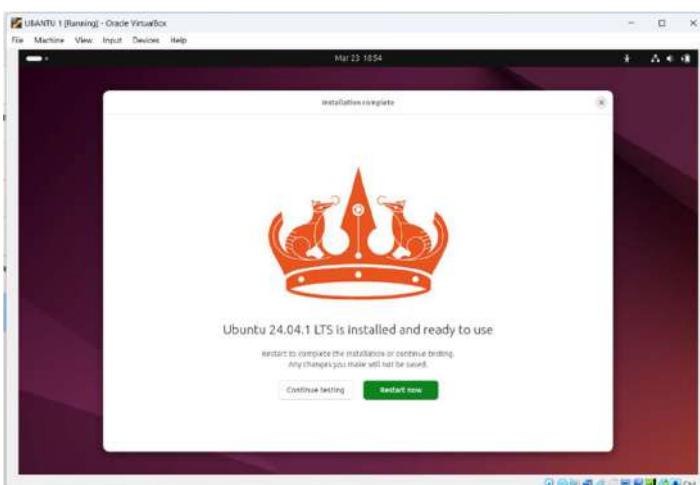
Then Click **Next**.



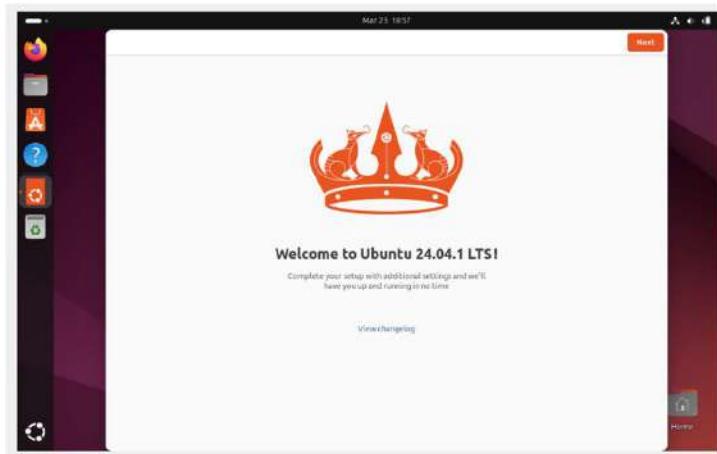
Then Click **Install**.



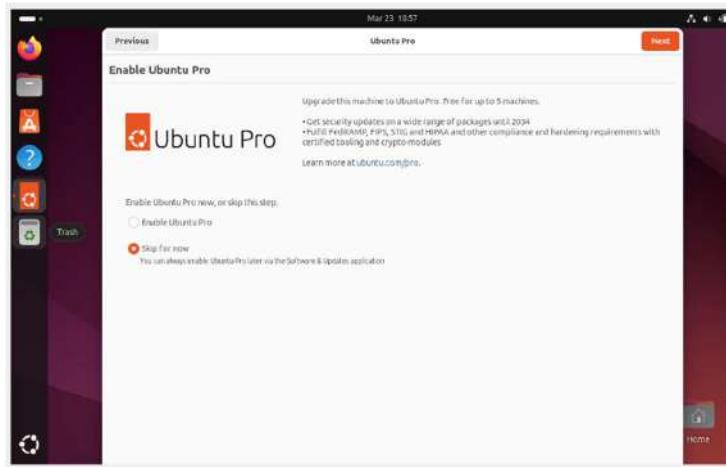
After Installation click on **Restart**.



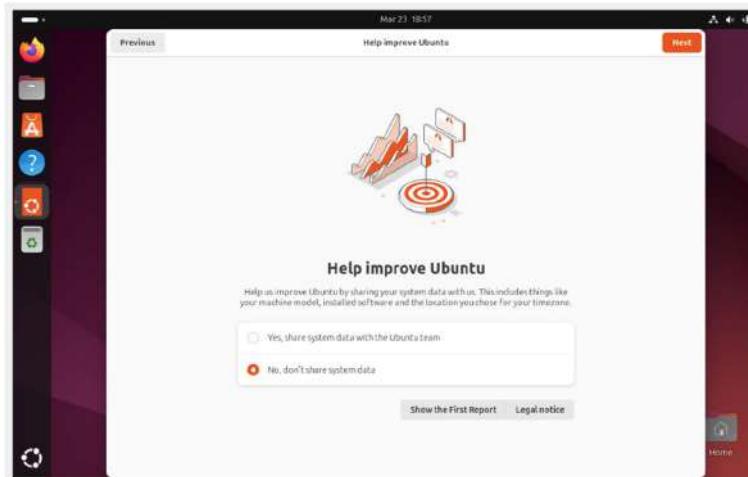
Then Click **Next**.



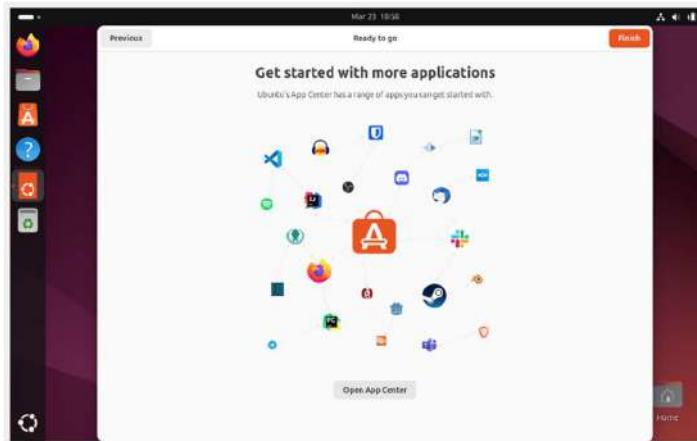
Click **Next**.



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

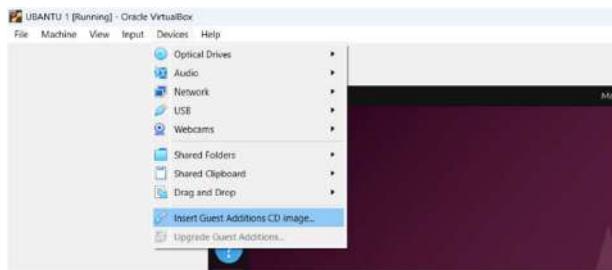


Click on **Finish**.



## 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.

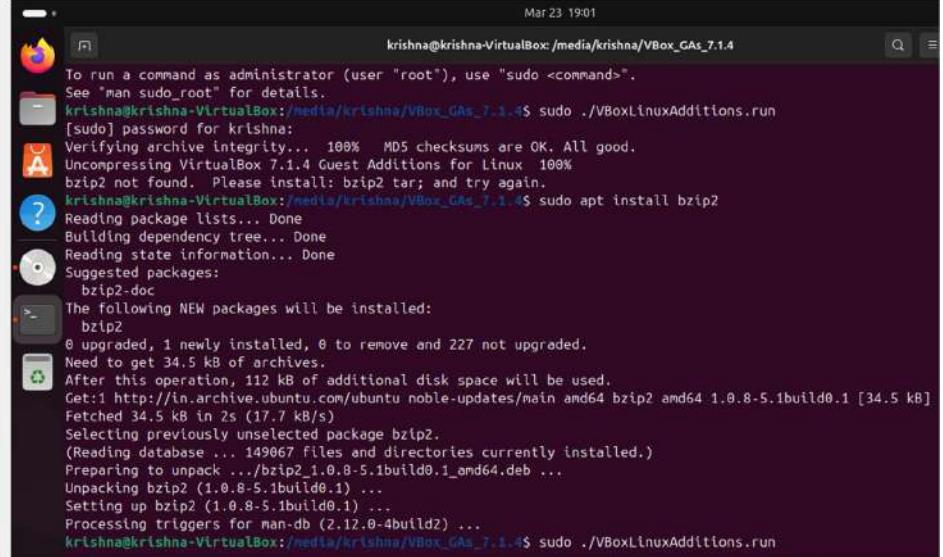
Right-click anywhere in the empty area in the File Explorer and select “[Open in Terminal](#)”.



Run the following command to install Guest Additions:

```
sudo ./VBoxLinuxAdditions.run
```

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



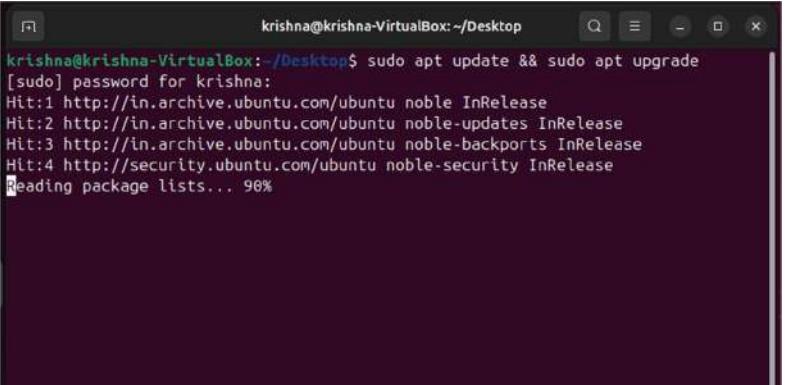
```
Mar 23 19:01
krishna@krishna-VirtualBox:~/media/krishna/VBox_GAs_7.1.4$ sudo ./VBoxLinuxAdditions.run
[sudo] password for krishna:
Verifying archive integrity... 100% MD5 checksums are OK. All good.
bztp2 not found. Please install: bztp2.tar; and try again.
krishna@krishna-VirtualBox:~/media/krishna/VBox_GAs_7.1.4$ sudo apt install bztp2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Suggested packages:
  bztp2-doc
The following NEW packages will be installed:
  bztp2
0 upgraded, 1 newly installed, 0 to remove and 227 not upgraded.
Need to get 34.5 kB of archives.
After this operation, 112 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 bztp2 amd64 1.0.8-5.1build0.1 [34.5 kB]
Fetched 34.5 kB in 2s (17.7 kB/s)
Selecting previously unselected package bztp2.
(Reading database ... 149067 files and directories currently installed.)
Preparing to unpack .../bztp2_1.0.8-5.1build0.1_amd64.deb ...
Unpacking bztp2 (1.0.8-5.1build0.1) ...
Setting up bztp2 (1.0.8-5.1build0.1) ...
Processing triggers for man-db (2.12.0-4build2) ...
krishna@krishna-VirtualBox:~/media/krishna/VBox_GAs_7.1.4$ sudo ./VBoxLinuxAdditions.run
```

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
```



```
krishna@krishna-VirtualBox:~/Desktop$ sudo apt update && sudo apt upgrade
[sudo] password for krishna:
Hit:1 http://in.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... 90%
```

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):

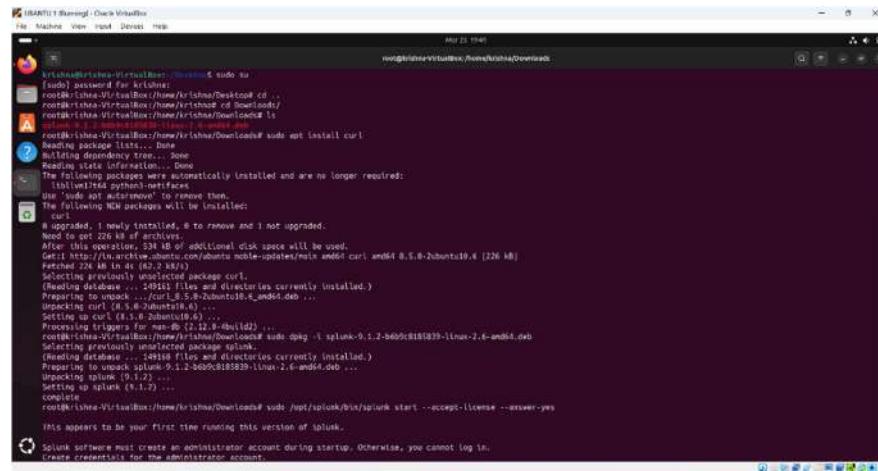
**sudo apt install curl**

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.



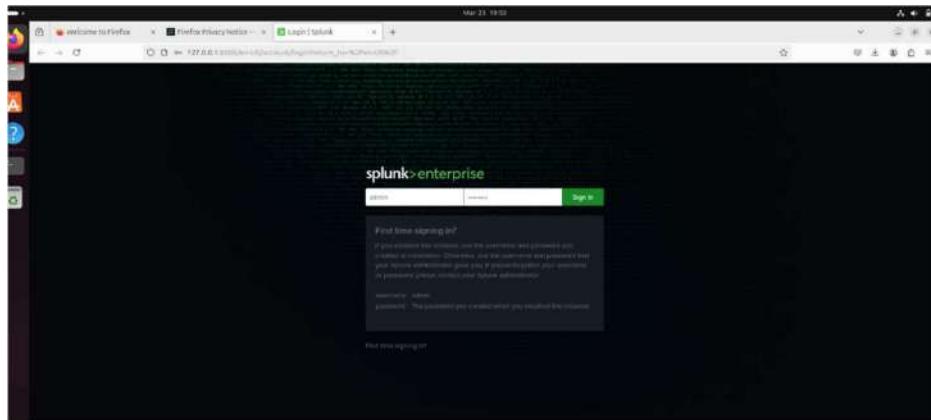
Once the setup is complete we see the Splunk is running on **http://127.0.0.1:8000**



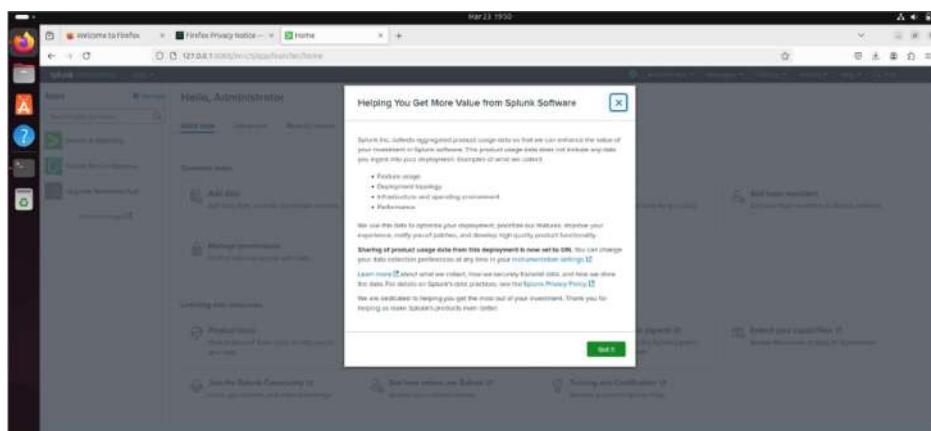
Run the following to allow Splunk to start automatically when the system is booted.

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

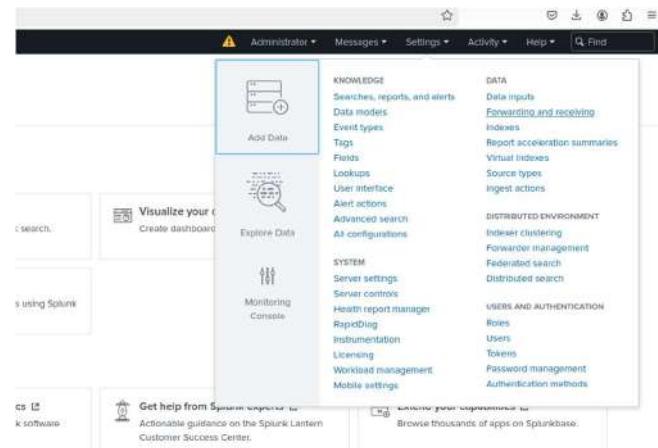
Before we can install Splunk Universal Forwarder there are a few settings we need to change in Splunk. Open Splunk by going to **http://127.0.0.1:8000**.



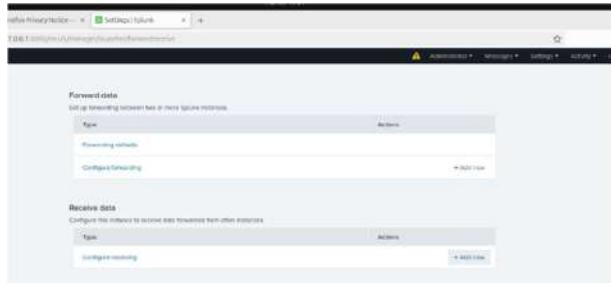
Click on **got it**.



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**.

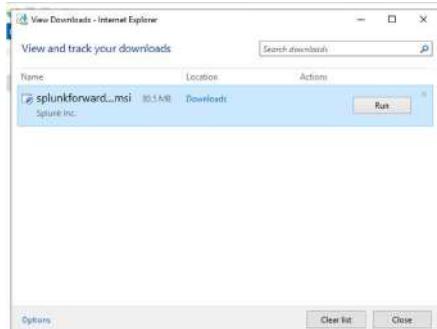


The next steps need to be performed on the Domain Controller (Windows Server 2019). We are going to ingest the log data that is generated by this device into Splunk.

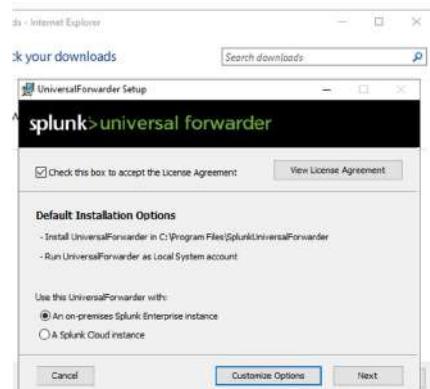
Go to the following link to download Universal Forwarder: [Download Universal Forwarder for Remote Data Collection | Splunk](#)

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.

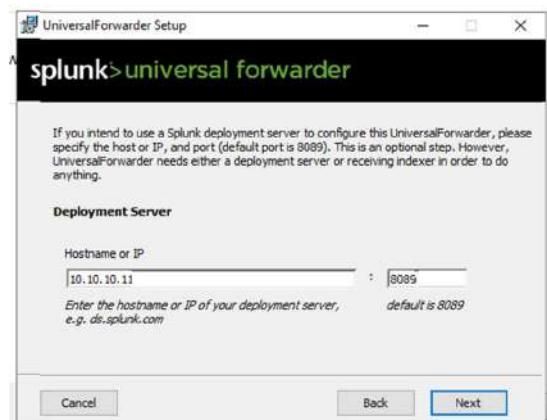


For the new step need the IP address of the Ubuntu (Splunk) VM. Use the following command to get the IP address.

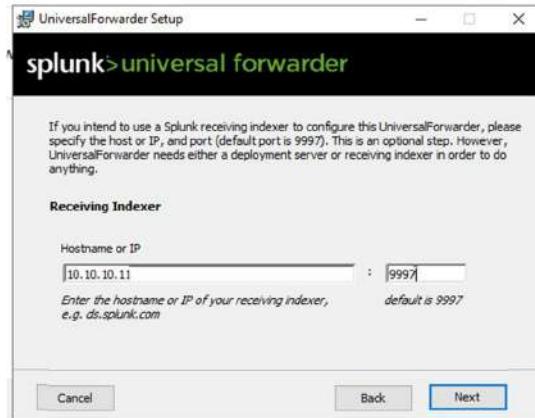
```
ip a
```

```
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#
```

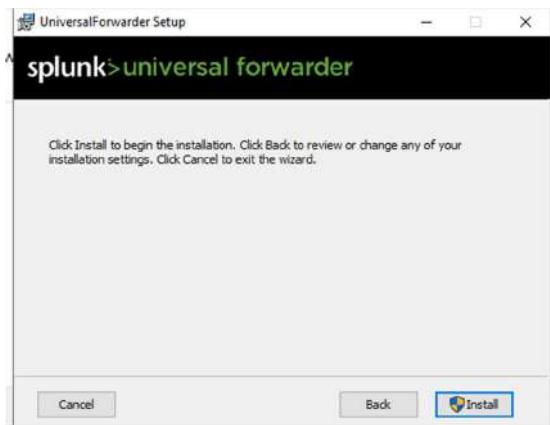
Enter the IP address of the Splunk VM (in my case **10.10.10.13**) and enter **8089** as the value for the port field then click on **Next**.



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**.

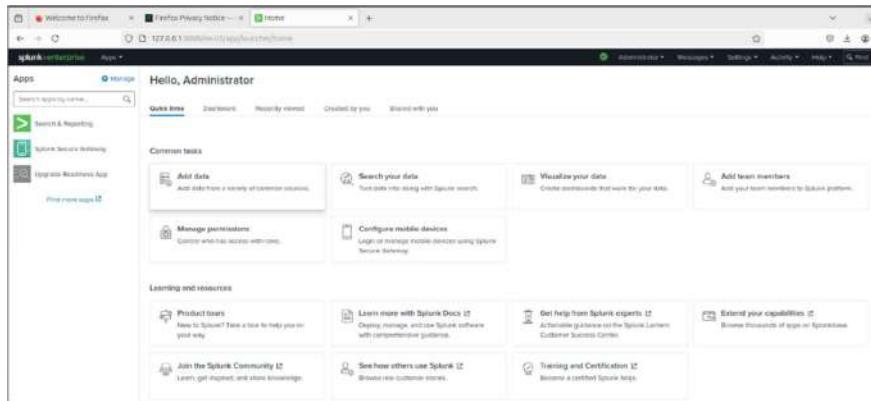


Click on **Finish** to close the installer.

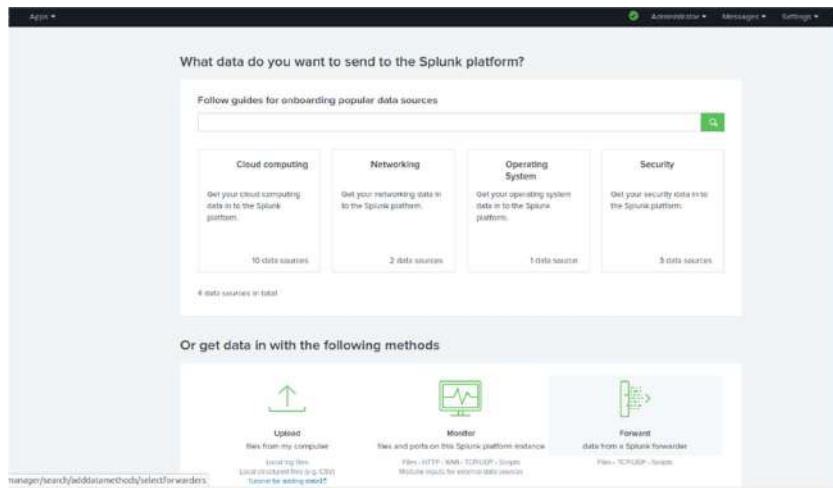


Now that we have Splunk and Universal Forwarder configured we need to link both the pieces together so that Splunk can collect data.

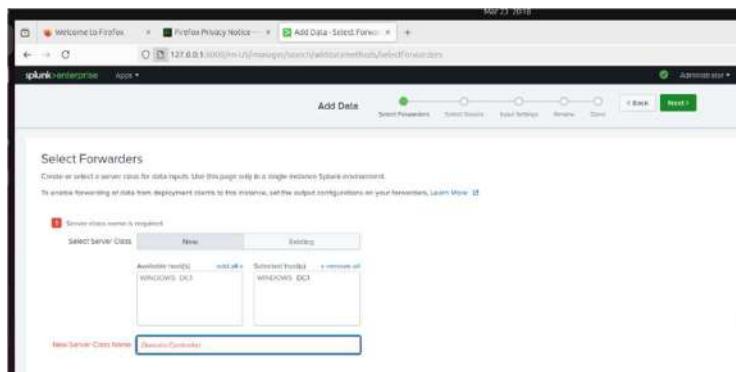
In Splunk select **Settings -> Add Data**.



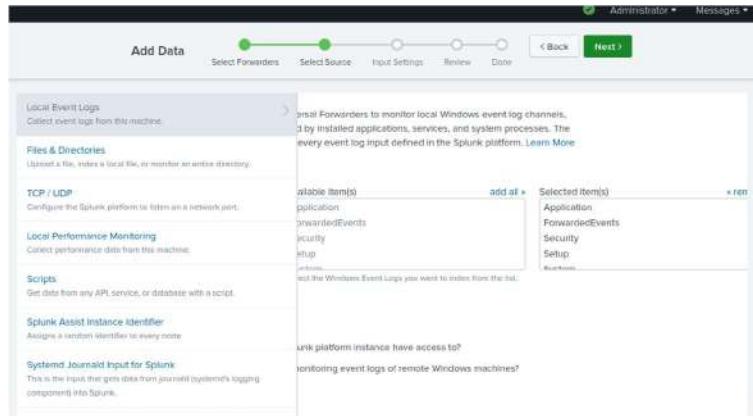
Click on **Forward**.



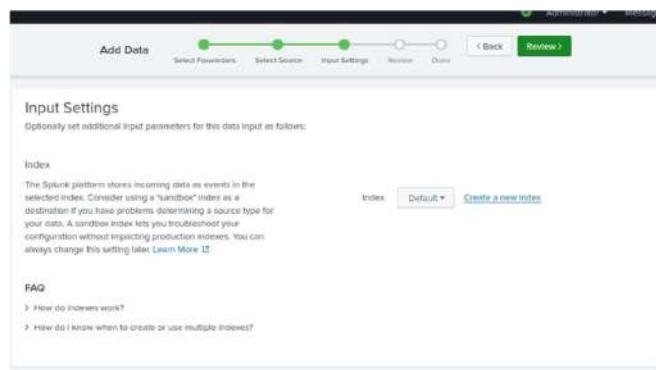
Our DC VM should automatically show up in the left box. Click on “add all” to move it to the right side. In the “New Source Class Name” field provide a name for the source. Click on **Next** to continue.



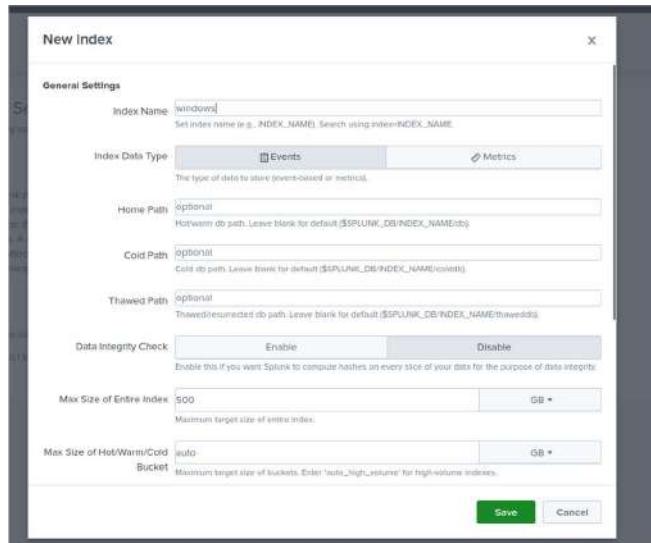
Select “Local Event Logs” then click on the “add all” button above the dropdown field to ingest all the logs generated by the DC. Click on **Next** once done.



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

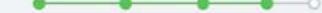


Provide the Index a name. Keep all the other fields on their default value and click on **Save** then click on **Next**.



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

Add Data



Administrator > Message

Review

Server Class Name: Domain Controller

List of Forwarders: WINDOWS 1 DC1

Collection Name: localhost

Input Type: Windows Event Logs

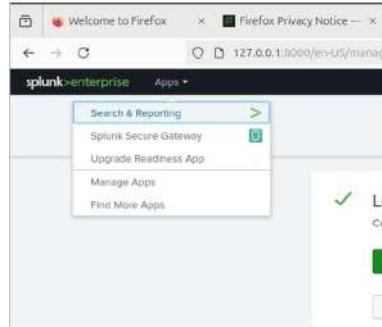
Event Logs: Application, ForwardedEvents, Security, Setup, System

Index: windows

< Back 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

New Search

Index="Windows"

1,860 events (02/23/2010 00:00 PM to 02/23/2010 02:00:00 PM) No Event Sampling

Events (1,860) Patterns Statistics Visualization

Format: `format` - `zoom out` `zoom in` `refresh` `clear`

Events per second

Time Event

3/23/2010 01:59:14 AM

LogonEvent: 81-00-14-AB

EventCode=7038

EventID=7038

EventTime=4

EventUser=SC1-81-00-14-AB

Source=All Drives

host=DC1 source=WEventLog System sourcetype=WEventLog System

3/23/2010 01:59:06 AM

LogonEvent: 81-00-14-AB

EventCode=7038

EventID=7038

EventTime=4

EventUser=SC1-81-00-14-AB

Source=All Drives

host=DC1 source=WEventLog System sourcetype=WEventLog System

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 229 230 231 232 233 234 235 236 237 238 239 239 240 241 242 243 244 245 246 247 248 249 249 250 251 252 253 254 255 256 257 258 259 259 260 261 262 263 264 265 266 267 268 269 269 270 271 272 273 274 275 276 277 278 279 279 280 281 282 283 284 285 286 287 288 289 289 290 291 292 293 294 295 296 297 298 299 299 300 301 302 303 304 305 306 307 308 309 309 310 311 312 313 314 315 316 317 318 319 319 320 321 322 323 324 325 326 327 328 329 329 330 331 332 333 334 335 336 337 338 339 339 340 341 342 343 344 345 346 347 348 349 349 350 351 352 353 354 355 356 357 358 359 359 360 361 362 363 364 365 366 367 368 369 369 370 371 372 373 374 375 376 377 378 379 379 380 381 382 383 384 385 386 387 388 389 389 390 391 392 393 394 395 396 397 398 399 399 400 401 402 403 404 405 406 407 408 409 409 410 411 412 413 414 415 416 417 418 419 419 420 421 422 423 424 425 426 427 428 429 429 430 431 432 433 434 435 436 437 438 439 439 440 441 442 443 444 445 446 447 448 449 449 450 451 452 453 454 455 456 457 458 459 459 460 461 462 463 464 465 466 467 468 469 469 470 471 472 473 474 475 476 477 478 479 479 480 481 482 483 484 485 486 487 488 489 489 490 491 492 493 494 495 496 497 498 499 499 500 501 502 503 504 505 506 507 508 509 509 510 511 512 513 514 515 516 517 518 519 519 520 521 522 523 524 525 526 527 528 529 529 530 531 532 533 534 535 536 537 538 539 539 540 541 542 543 544 545 546 547 548 549 549 550 551 552 553 554 555 556 557 558 559 559 560 561 562 563 564 565 566 567 568 569 569 570 571 572 573 574 575 576 577 578 579 579 580 581 582 583 584 585 586 587 588 589 589 590 591 592 593 594 595 596 597 598 599 599 600 601 602 603 604 605 606 607 608 609 609 610 611 612 613 614 615 616 617 618 619 619 620 621 622 623 624 625 626 627 628 629 629 630 631 632 633 634 635 636 637 638 639 639 640 641 642 643 644 645 646 647 648 649 649 650 651 652 653 654 655 656 657 658 659 659 660 661 662 663 664 665 666 667 668 669 669 670 671 672 673 674 675 676 677 678 679 679 680 681 682 683 684 685 686 687 688 689 689 690 691 692 693 694 695 696 697 698 699 699 700 701 702 703 704 705 706 707 708 709 709 710 711 712 713 714 715 716 717 718 719 719 720 721 722 723 724 725 726 727 728 729 729 730 731 732 733 734 735 736 737 738 739 739 740 741 742 743 744 745 746 747 748 749 749 750 751 752 753 754 755 756 757 758 759 759 760 761 762 763 764 765 766 767 768 769 769 770 771 772 773 774 775 776 777 778 779 779 780 781 782 783 784 785 786 787 788 789 789 790 791 792 793 794 795 796 797 798 799 799 800 801 802 803 804 805 806 807 808 809 809 810 811 812 813 814 815 816 817 818 819 819 820 821 822 823 824 825 826 827 828 829 829 830 831 832 833 834 835 836 837 838 839 839 840 841 842 843 844 845 846 847 848 849 849 850 851 852 853 854 855 856 857 858 859 859 860 861 862 863 864 865 866 867 868 869 869 870 871 872 873 874 875 876 877 878 879 879 880 881 882 883 884 885 886 887 888 889 889 890 891 892 893 894 895 896 897 898 899 899 900 901 902 903 904 905 906 907 908 909 909 910 911 912 913 914 915 916 917 918 919 919 920 921 922 923 924 925 926 927 928 929 929 930 931 932 933 934 935 936 937 938 939 939 940 941 942 943 944 945 946 947 948 949 949 950 951 952 953 954 955 956 957 958 959 959 960 961 962 963 964 965 966 967 968 969 969 970 971 972 973 974 975 976 977 978 979 979 980 981 982 983 984 985 986 987 988 989 989 990 991 992 993 994 995 996 997 998 999 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2099 2100 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2199 2200 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2299 2300 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2379 2380 2381 2382 2383 2384

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