### **SOC Home Lab Setup**

This is a detailed step by step guide on how I created an Active Directory lab at home.

#### **Part-1: Virtual Machine Installation**

#### **Network Overview**

In this carefully designed home lab environment, I’ve set up a comprehensive network infrastructure that simulates a small enterprise network while incorporating security monitoring and analysis tools.

#### **Network Configuration**

* **Domain**: Home Domain
* **Network Range**: 192.168.10.0/24
* **Total Devices**: 4 key systems

#### **Key Components**

#### **1. Network Router/Switch**

* Central networking device
* Connects all lab components
* Provides internet connectivity
* Enables communication between different network segments

#### **2. Active Directory Server**

* **IP Address**: 192.168.10.7
* Runs Windows Server
* Responsible for:
* User authentication
* Network policy management
* Domain controller functionality
* Hosts Sysmon for advanced system monitoring

#### **3. Splunk Infrastructure**

* **Splunk Server IP**: 192.168.10.10
* Runs Splunk Universal Forwarder
* Central log management and security information and event management (SIEM) system
* Collects and analyzes logs from multiple sources

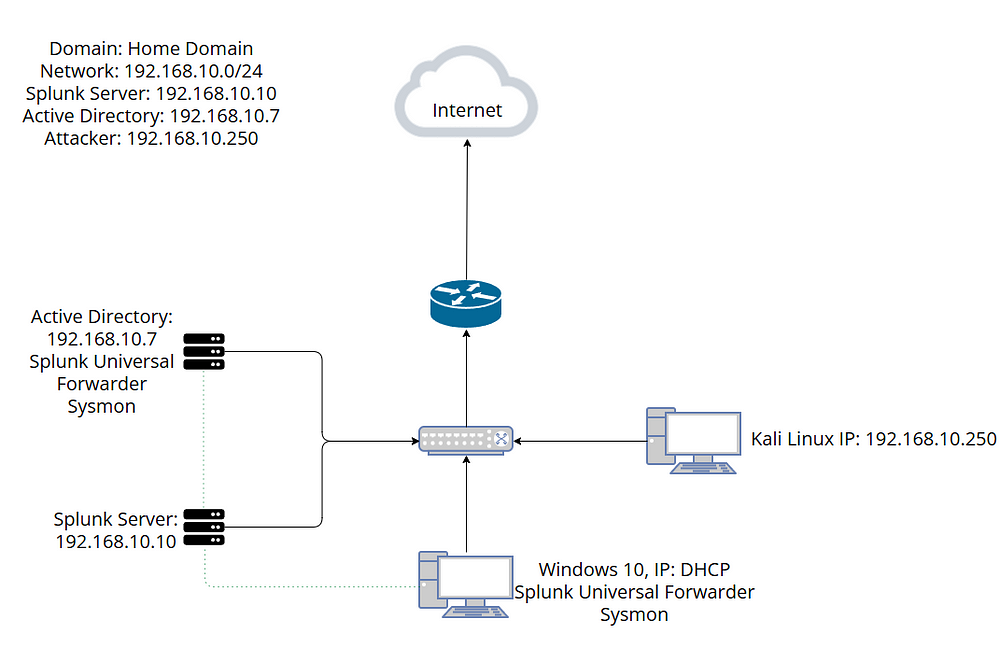
#### **4. Client Machines**

#### **Windows 10 Client**

* IP Address: Dynamically assigned via DHCP
* Runs Splunk Universal Forwarder
* Sysmon installed for detailed system event logging
* Represents a typical enterprise workstation

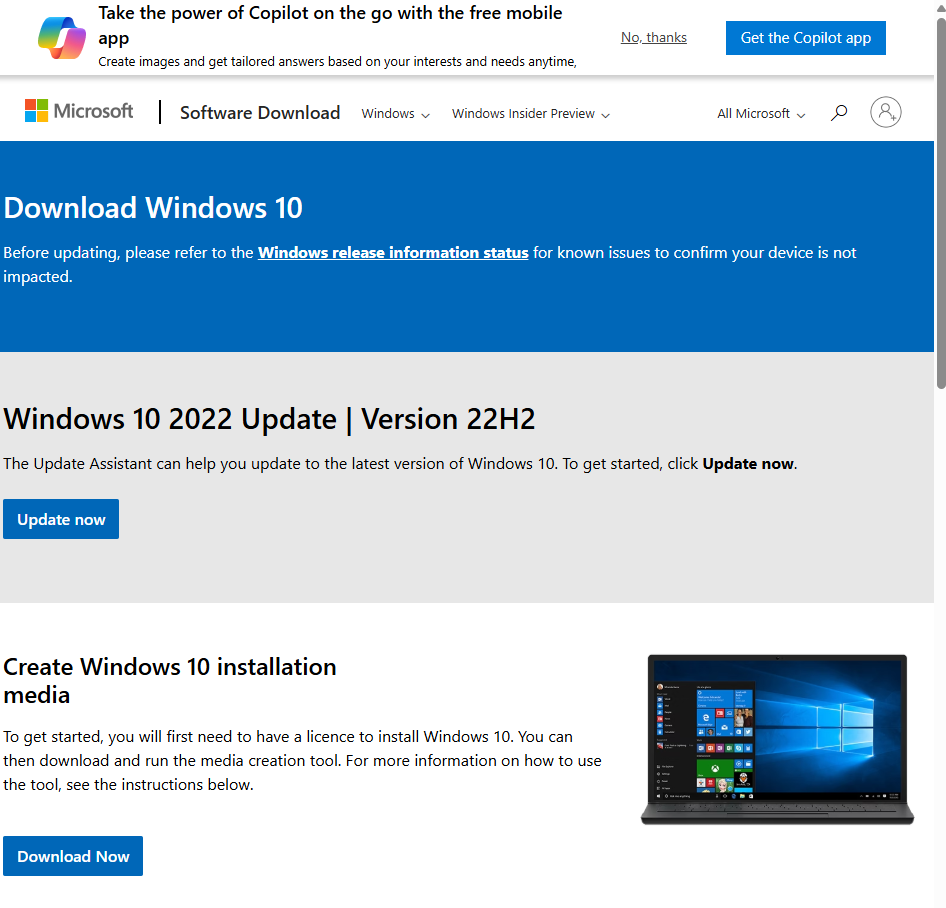
#### **Kali Linux Machine**

* **IP Address**: 192.168.10.250
* Cybersecurity-focused distribution
* Used for penetration testing and security research
* Simulates an “attacker” perspective in this lab.

Network Diagram

#### **1.Windows-10 Installation**

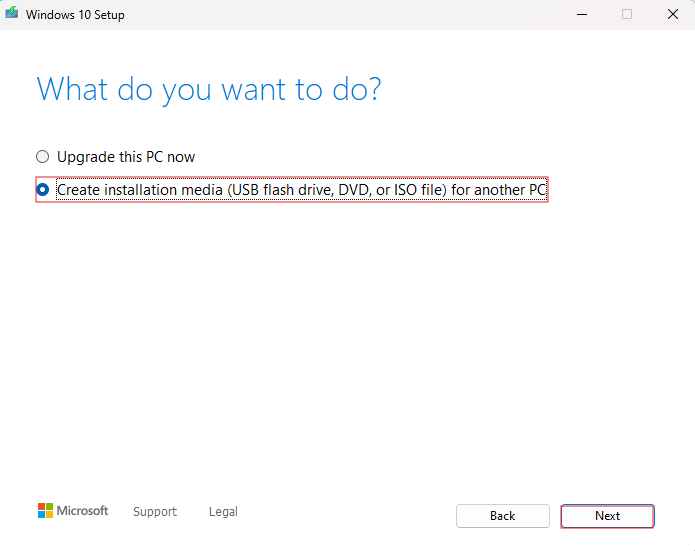
To download the Windows 10 iso image, we first need to download the Media creation tool which is available [here](https://www.microsoft.com/en-us/software-download/windows10).

Windows-10 download page

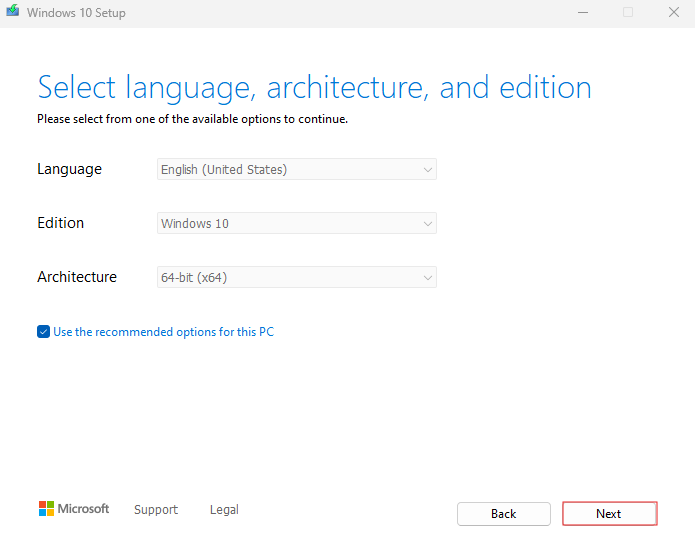
Once the tool is downloaded and run, the following screen appears. Select Accept.

Windows Media Creation tool

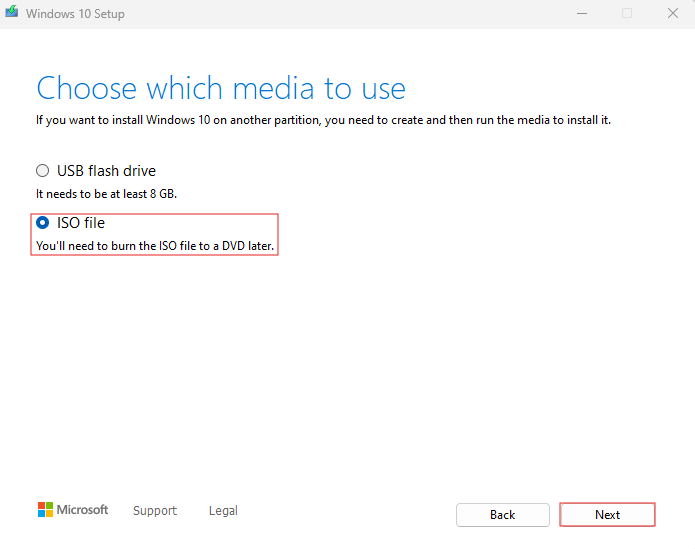
Next select the “Create installation media(USB flash drive, DVD, or ISO file)for another PC” option and click next.

Windows Media Creation tool

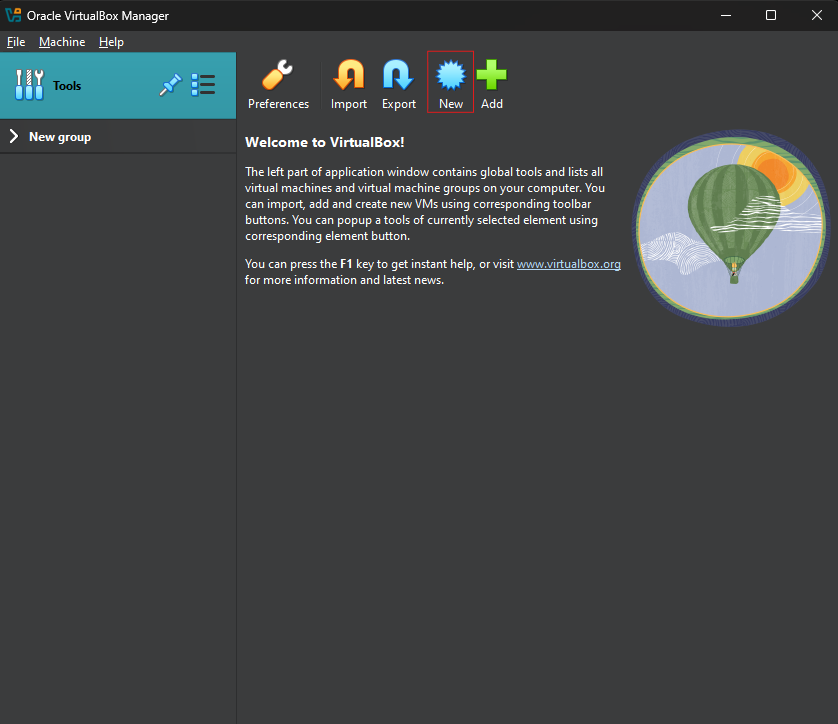
In the next screen select “use recommended options for this PC” and click next.

Windows Media Creation tool

Next, choose the “ISO file” option and click next. Now the .iso file download will start.

Windows Media Creation tool

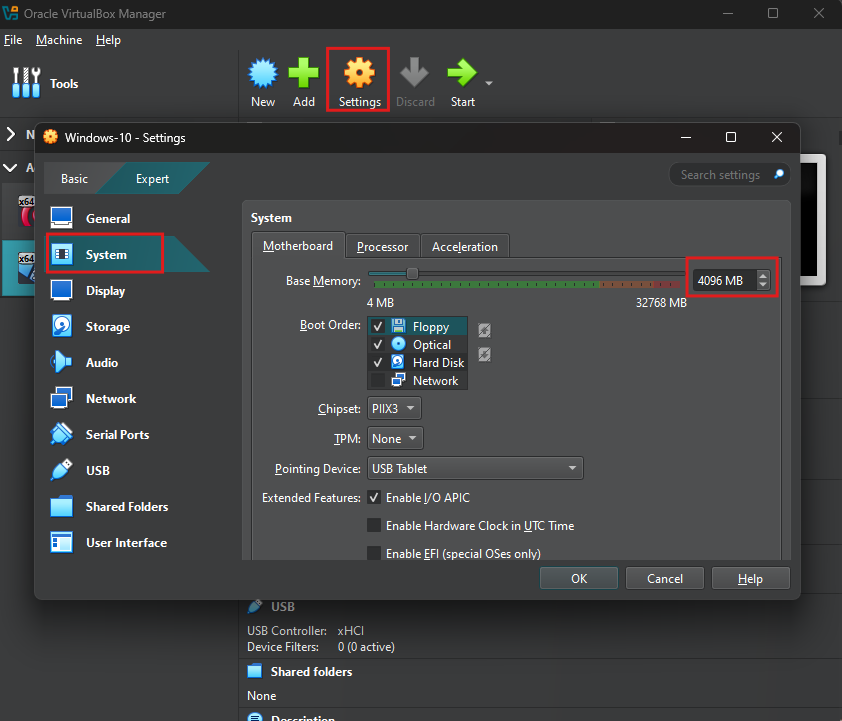
Once the .iso file is downloaded, we can open the virtual box and click on new.

Virtual Box

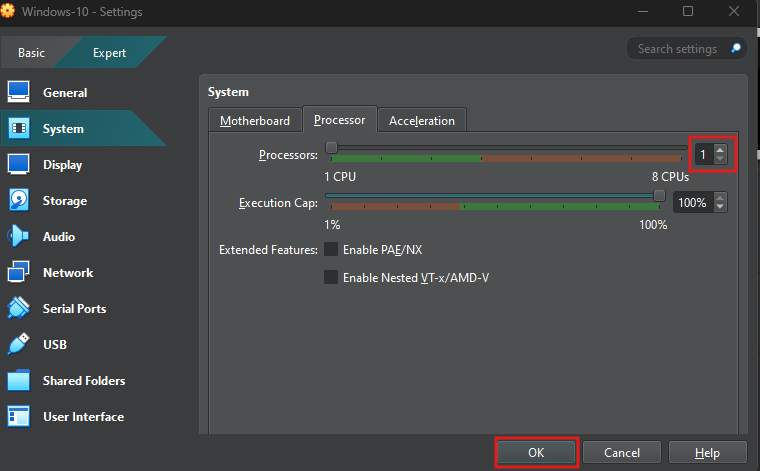
In the pop up enter the Virtual Machine name, select the path to the windows iso file and check the “Skip Unattended Installation” option and click finish.

Virtual Box

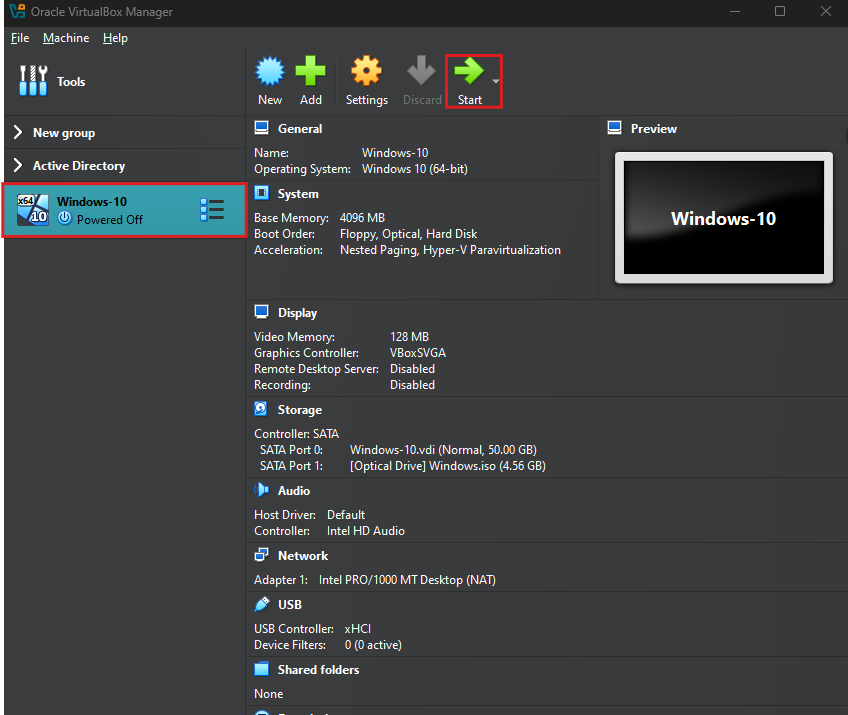
Now, go to settings->System and select the ram. Here I am selecting 4 Gb.

Virtual Machine settings

Now go to Processor settings and select number of processors, I left it to the default value. Now click Ok.

Virtual Machine settings

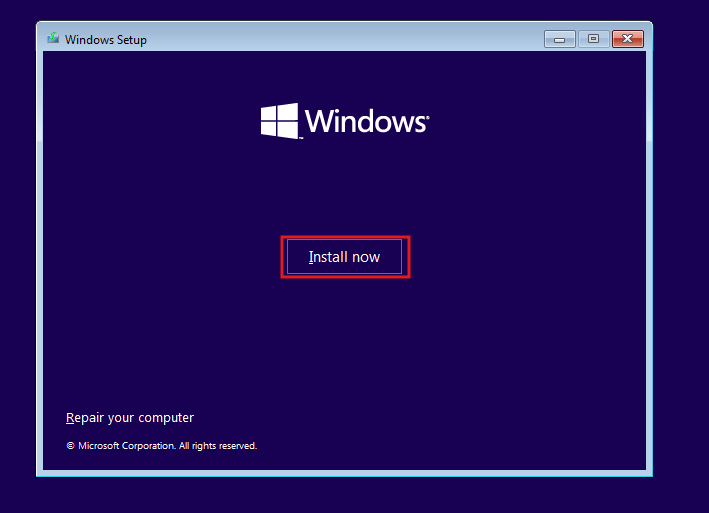
Now we can start the Virtual machine by selecting the virtual machine and clicking on start.

Virtual Box

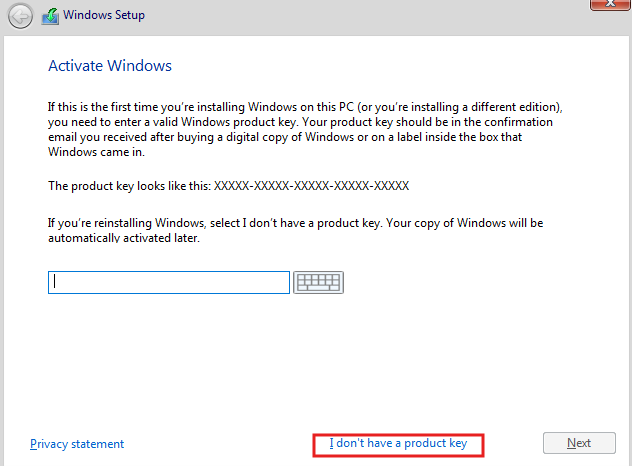
Now select the required options and click next.

Windows 10 setup

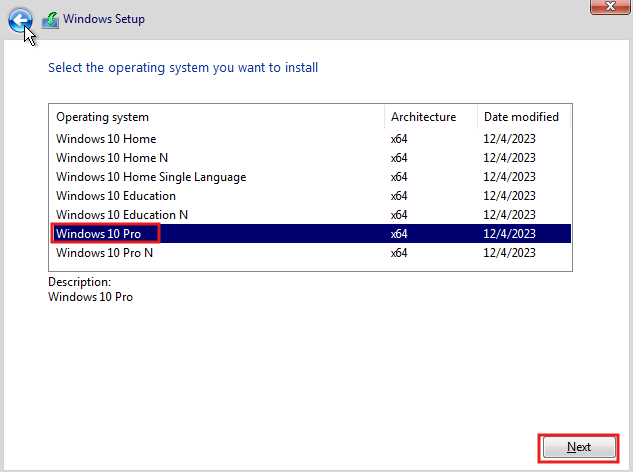
Then click on Install now.

Windows 10 setup

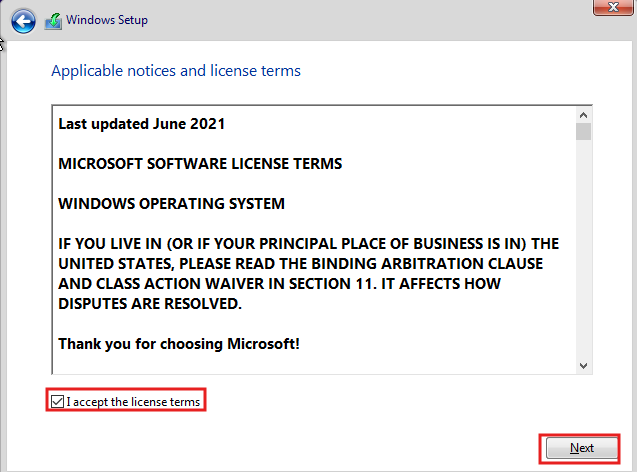
When prompted to enter the Windows activation key, click on “I don’t have a product key” option.

Windows 10 setup

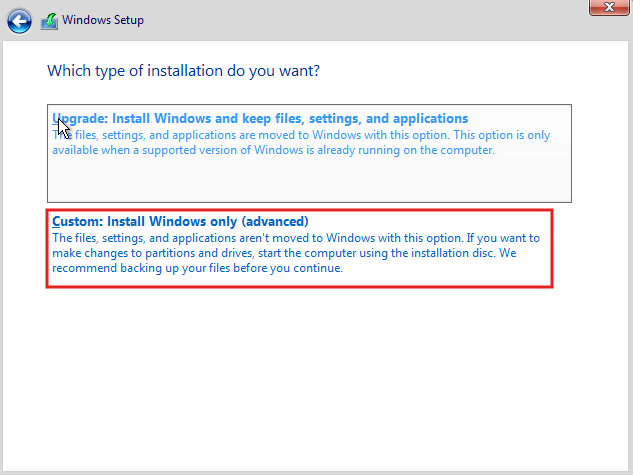
Then select Windows10 Pro and click Next.

Windows 10 setup

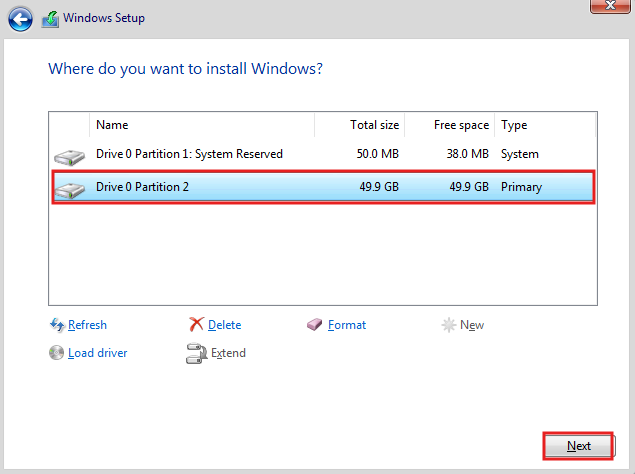
Then accept the terms and click Next.

Windows 10 setup

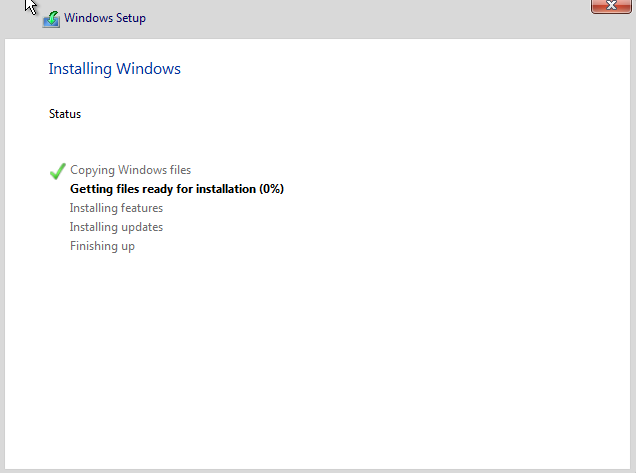
Then choose Custom: Install Windows only(advanced) option.

Windows 10 setup

Then click on new and apply, to create a new disk partition. It should look like the below screenshot. Then click Next.

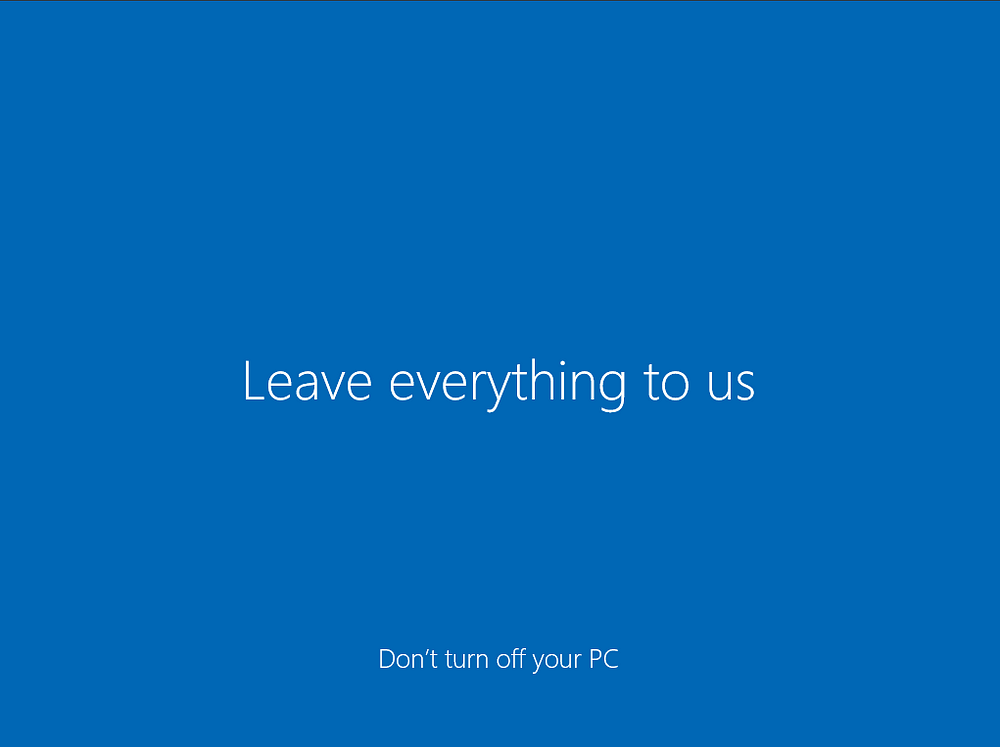
Windows 10 setup

Now the Windows installation will start, this might take some time based on the system.

Windows 10 setup

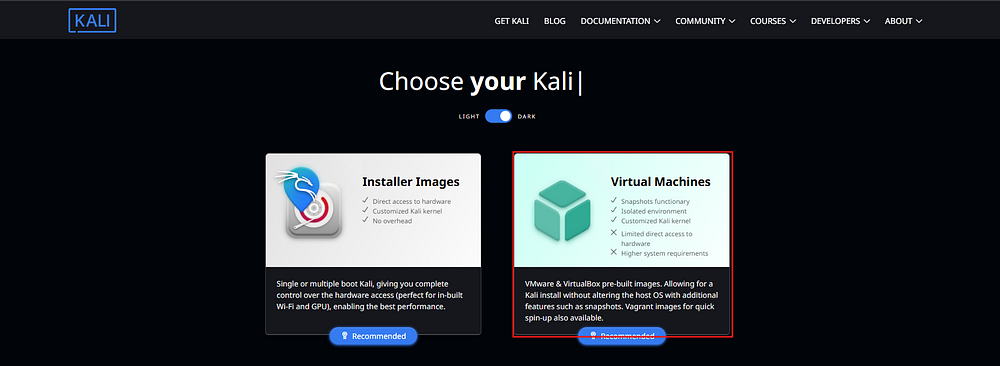
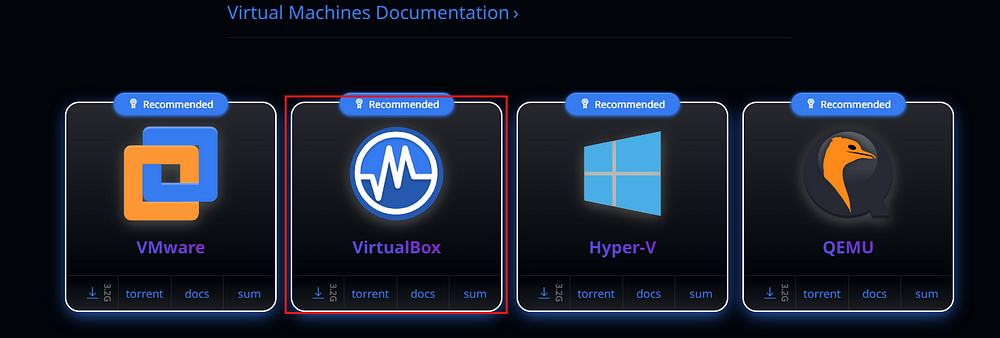
Once done this will prompt additional setup, select appropriate options.

Then when prompted to select the account type select as organizational and select domain join instead and complete the setup process. Once everything is done this screen will appear. Once this is complete the windows10 machince will be ready.

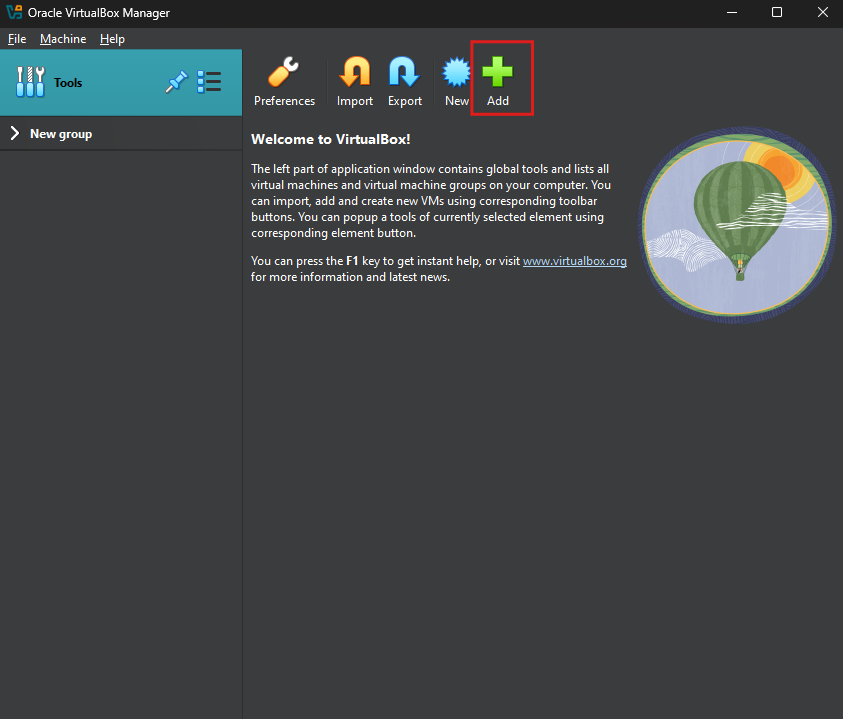
Windows 10 setup

#### **2.Kali Linux Installation**

For Kali Linux I chose the pre built virtual machine image available [here](https://www.kali.org/get-kali/#kali-platforms).

Kali DownloadKali VM image download

Once the image is downloaded we can directly add this to the virtual box by clicking on the Add button on the Vbox.

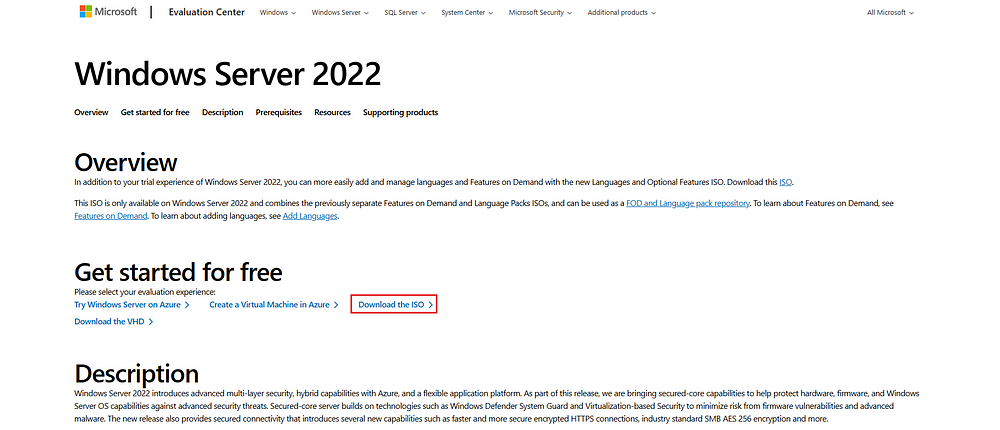
Adding Kali Linux virtual machine to VirtualBox

Select the downloaded vbox image and follow the simple installation steps. Now the Kali Linux machine will be ready.

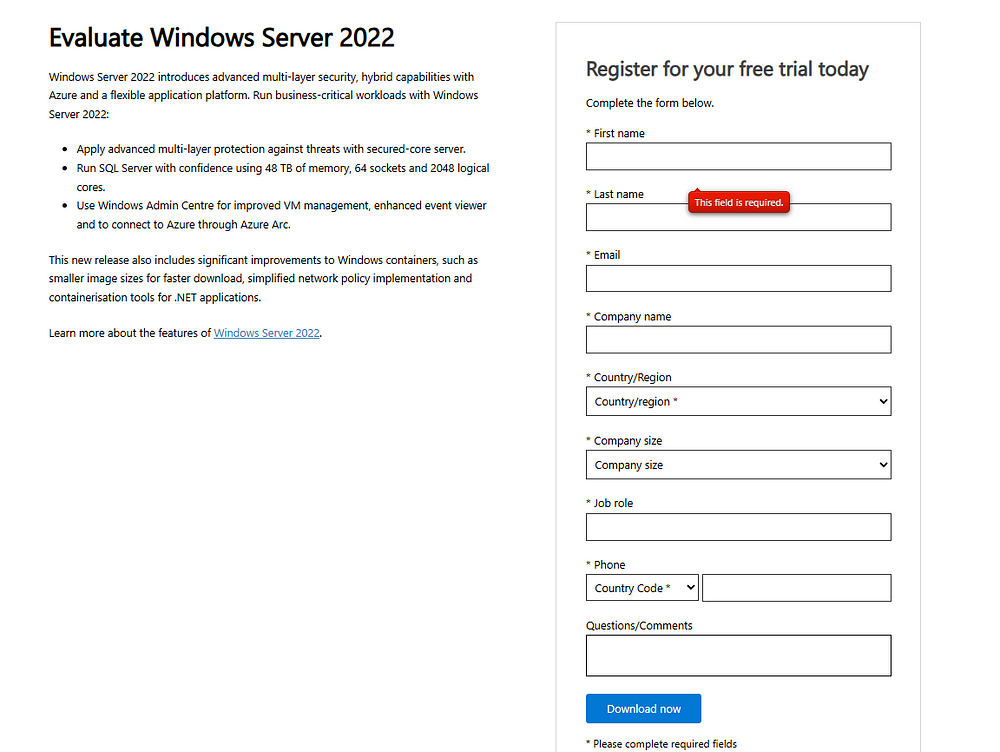
Kali Linux VM.

#### **3. Windows Server Installation**

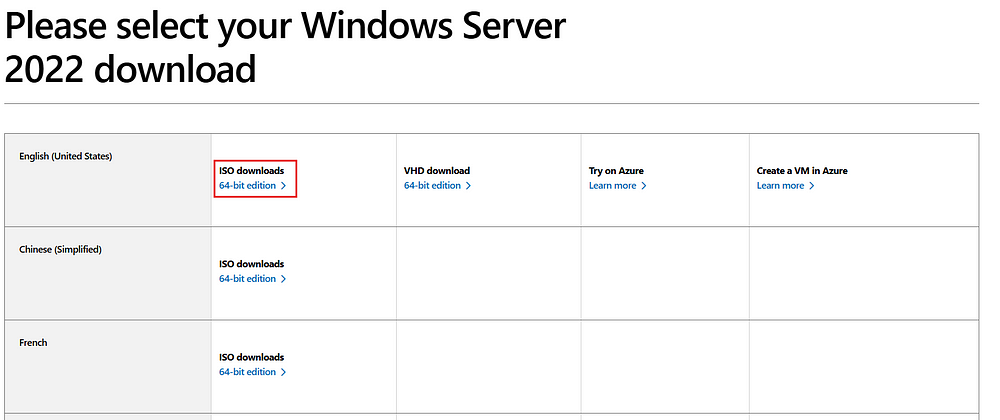
Now we can download the windows server image to setup the Active Directory domain controller. We can download the server image from [here](https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022). Once on the page click on the “Download the ISO” option as shown below.

Windows server image download.

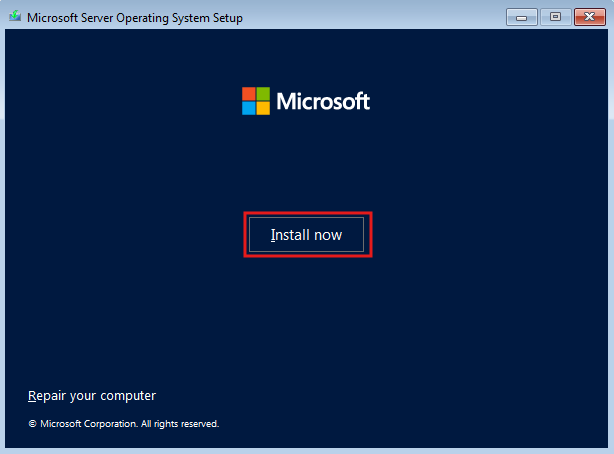
Once the option is clicked a new page opens where it asks to register for free trial. Fill in the details and click Download now.

Window server image download

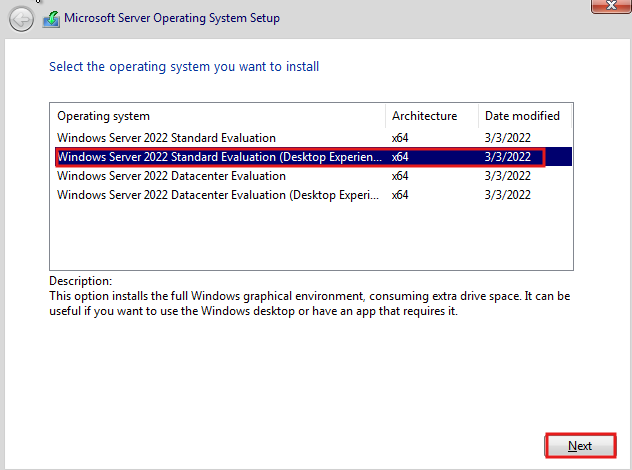
Then select the appropriate ISO. This will start the image download.

Window server image download.

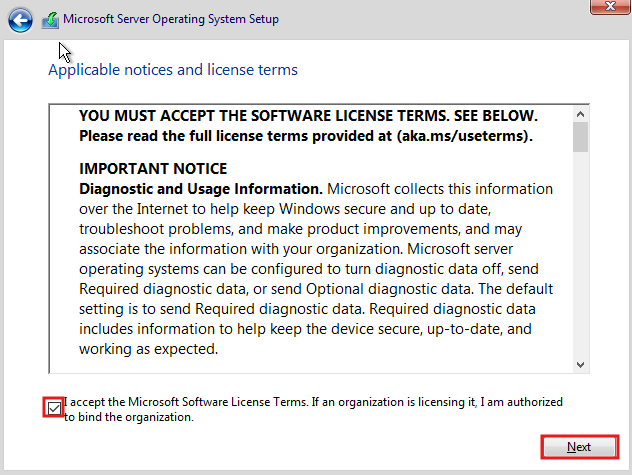
Once the image is downloaded we can setup the VM. To setup the VM please follow the same steps listed above for windows VM setup. Once all the settings were configured correctly we can start the VM. Once the VM is booted select the appropriate language and keyboadr options and then select install now.



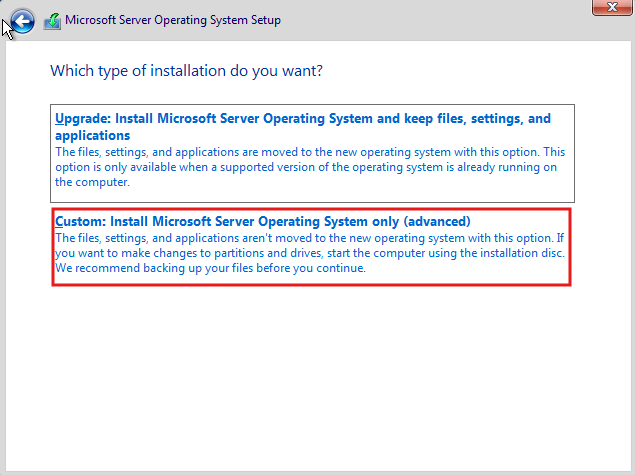
Next the following screen appears. Here select the “Windwos Server 2022 Standard Evaluation(Desktop Experience)” option and click next.

Windows server setup.

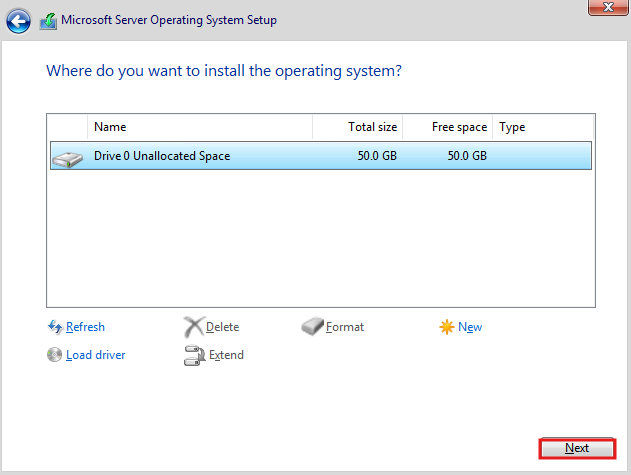
Accept the terms and continue.

Windows server setup.

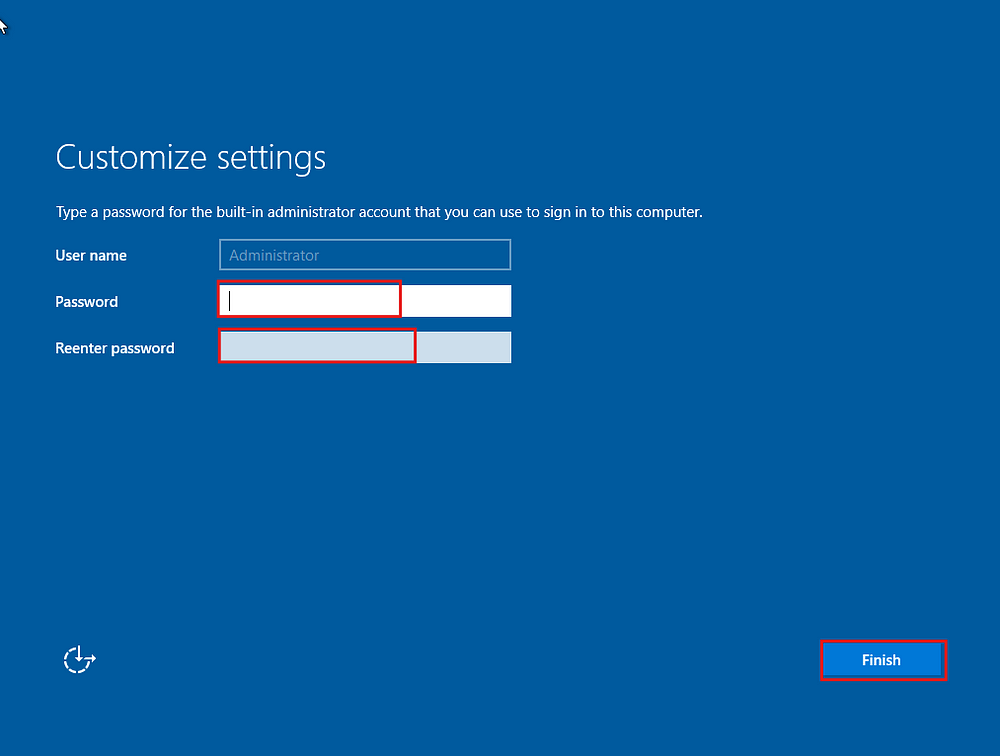
Then select Custom install.

Windows server setup.

Next we can leave the disk settings as it is and click next.

Windows server setup.

Now, setup a strong password and click finish.

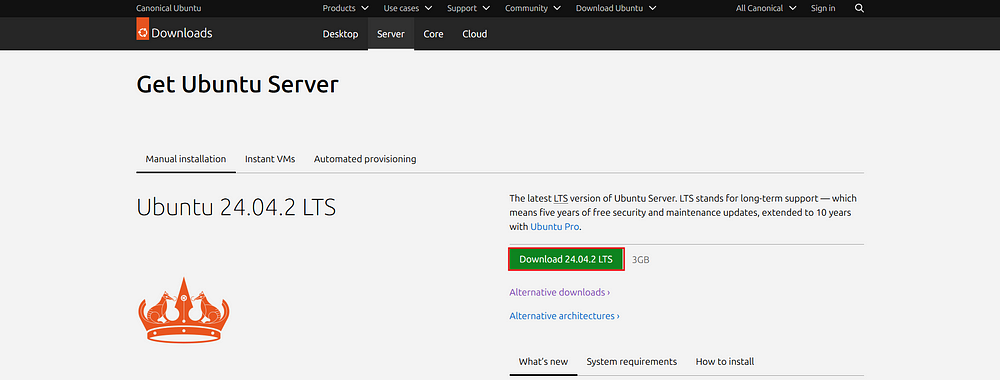
Windows server setup.

Once the system is installed It will prompt us to enter Ctrl+Alt+Del. To do this go to the virtual box menu on the top Input->Keyboard->Insert Ctrl + Alt + Del or just type windows key + Del.

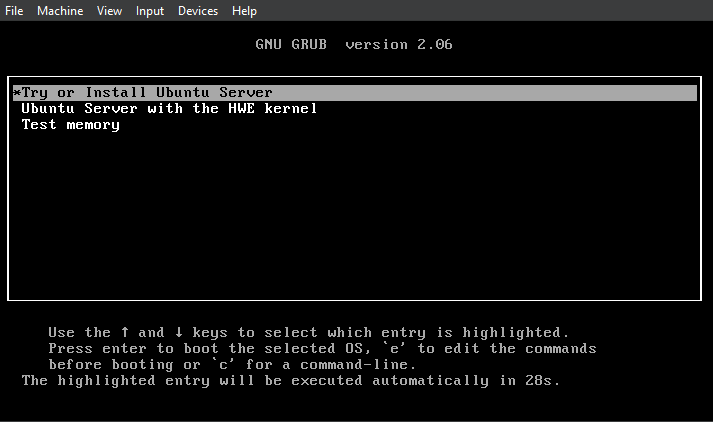
Windows server.

#### **4.Ubuntu Server Installation**

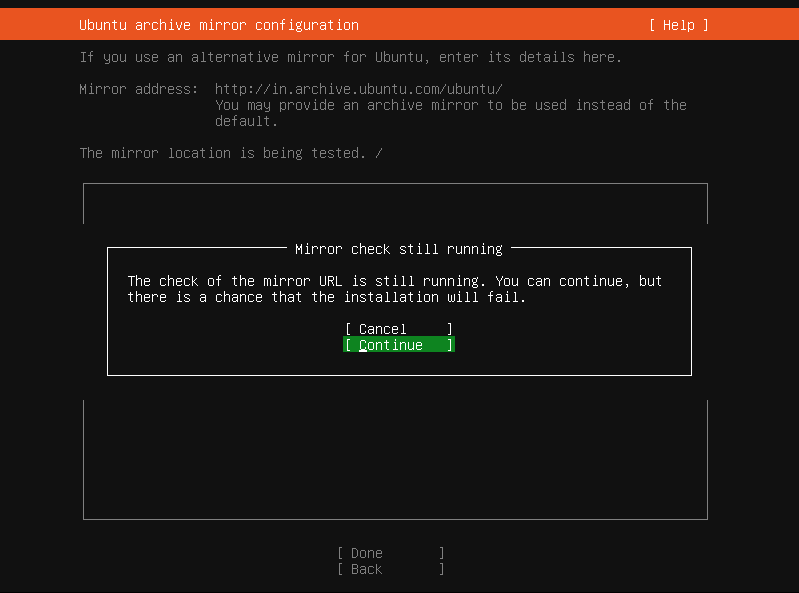
For Ubuntu server installation we can download the server image from [here](https://ubuntu.com/download/server). Download the latest server image.

Ubuntu server image download.

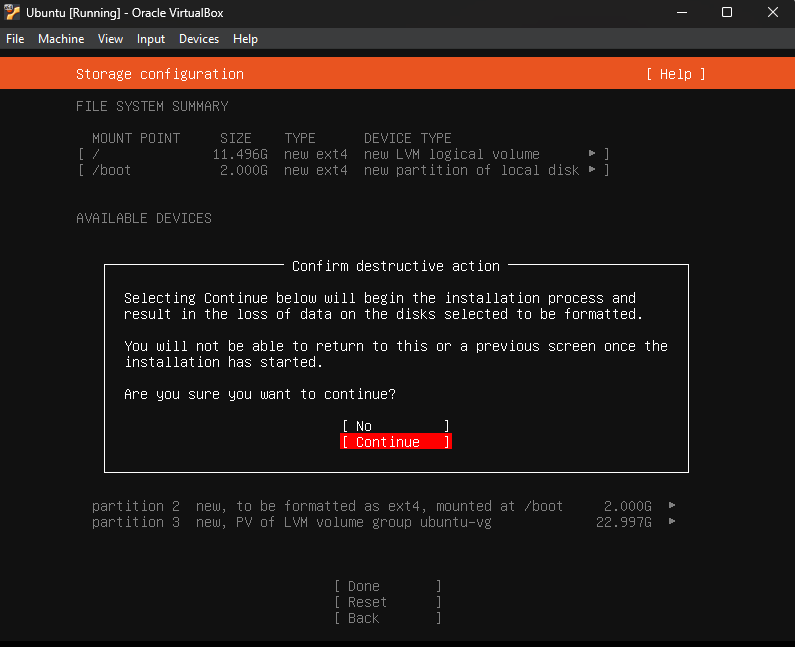
Then follow similar steps for virtual machine creation in virtual box as shown in the windows installation. Once we select the VM settings and start the VM the following option appears. Select Try or install Ubuntu Server option.

Ubuntu server installation.

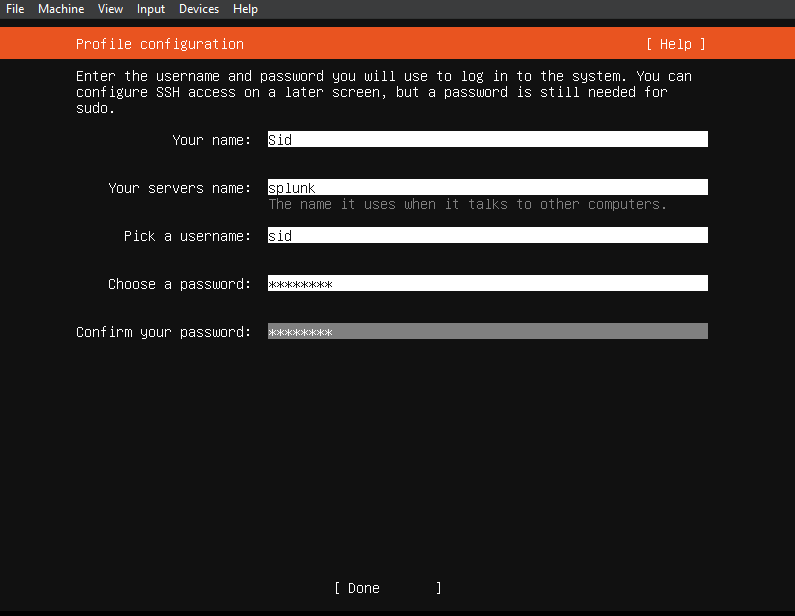
Then continue with default settings untill the following pop up appears. Here click continue.

Ubuntu server installation.

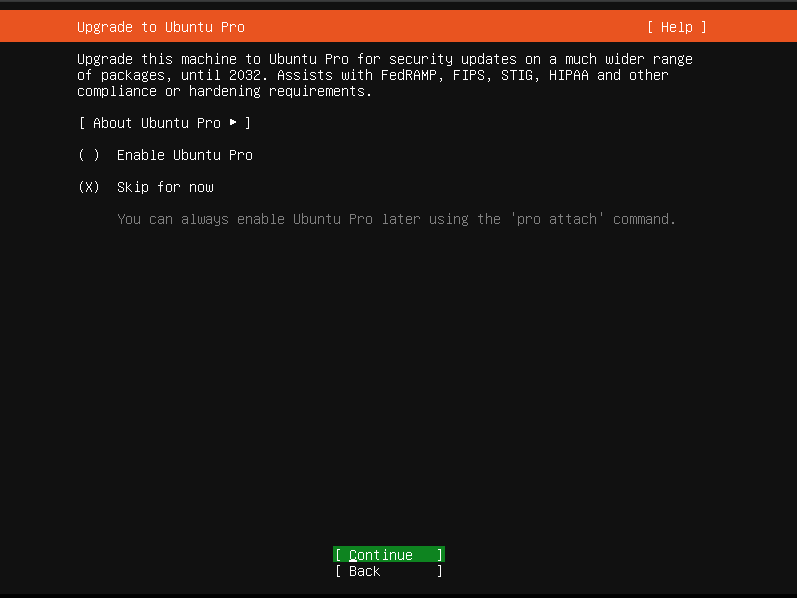
Then continue with default settings, then this pop up appears, here click continue.

Ubuntu server installation.

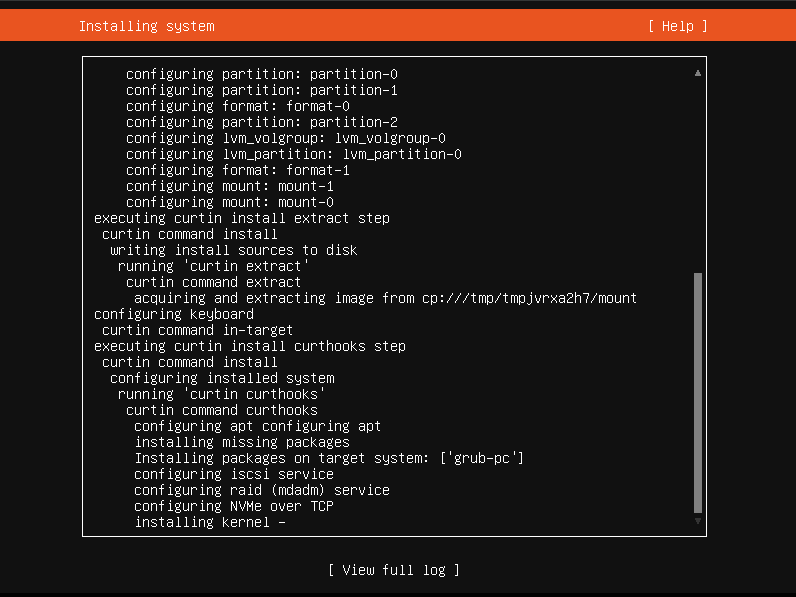
Then enter the name and other details and set a strong password and click Done.

Ubuntu server installation.

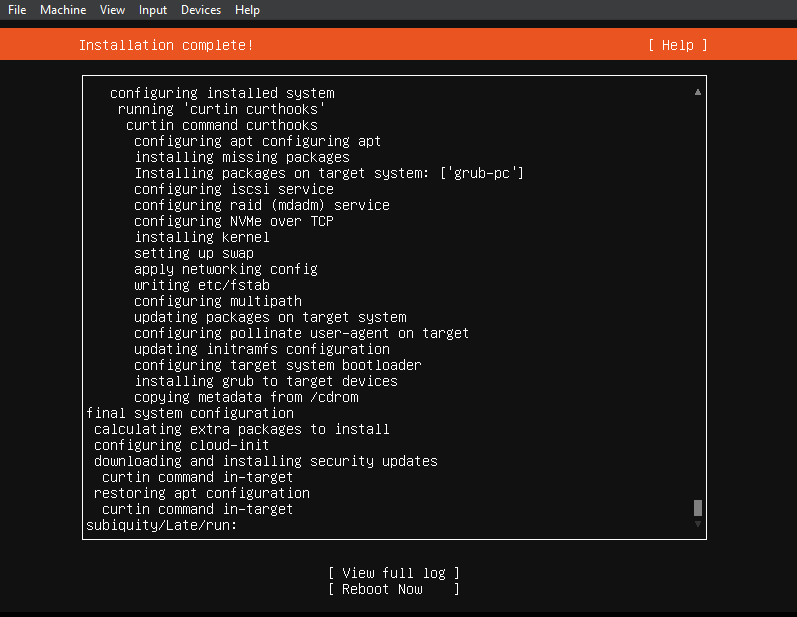
Then select skip for now on Ubuntu pro and cliock done.

Ubuntu server installation.

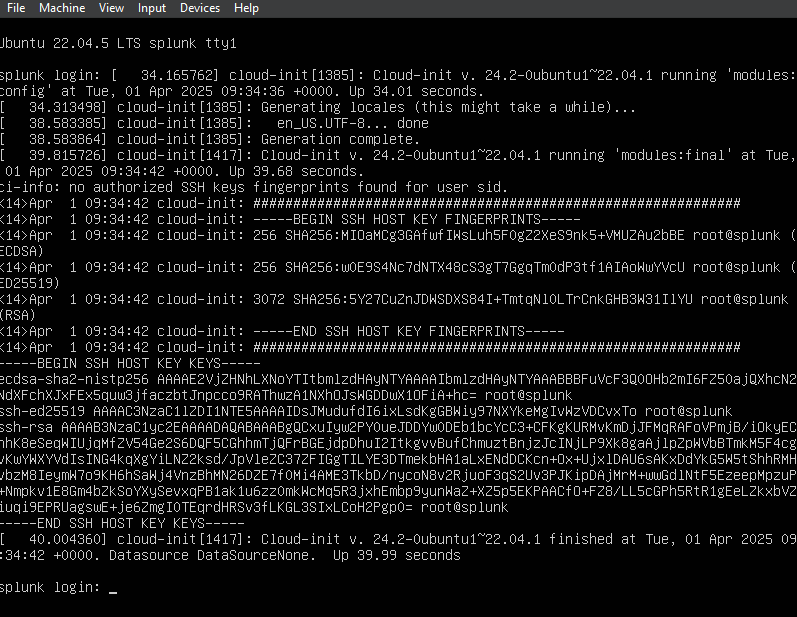
For the next steps just click continue or done without installing any additional settings. Then the system install will begin as shown below.

Ubuntu server installation.

Once the installation is complete, click Reboot Now.

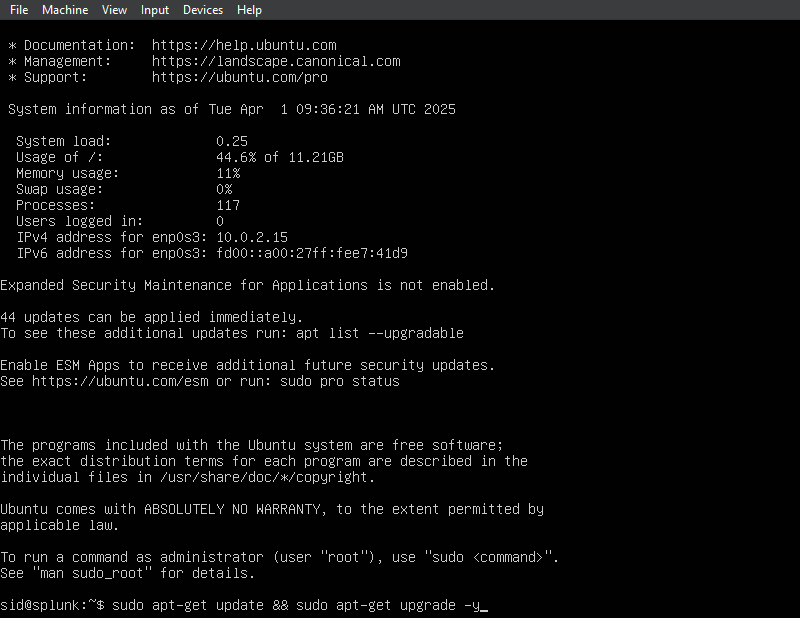
Ubuntu server installation.

Once the sustem reboots, we can login to our ubuntu server.

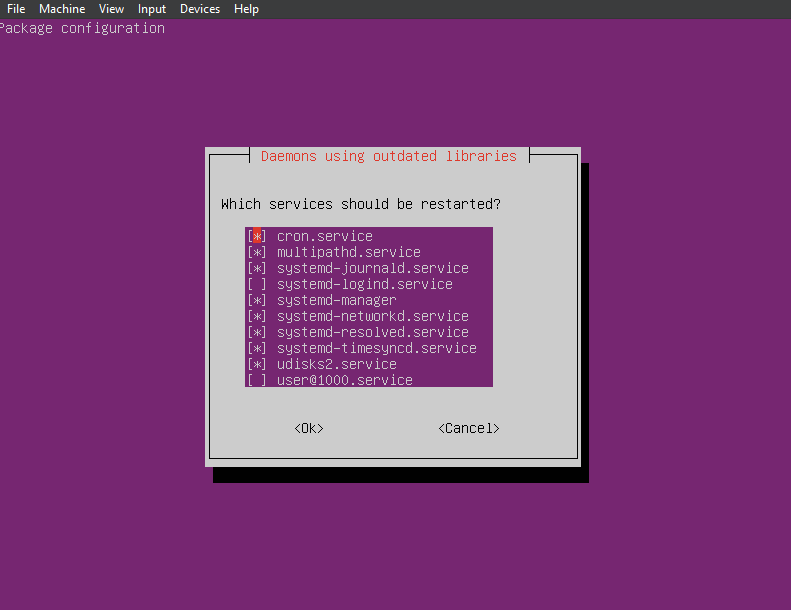
Ubuntu server installation.

Once logged in, run the following command. And enter your password when prompted.

sudo apt-get update && sudo apt-get upgrade -y

Ubuntu server installation.

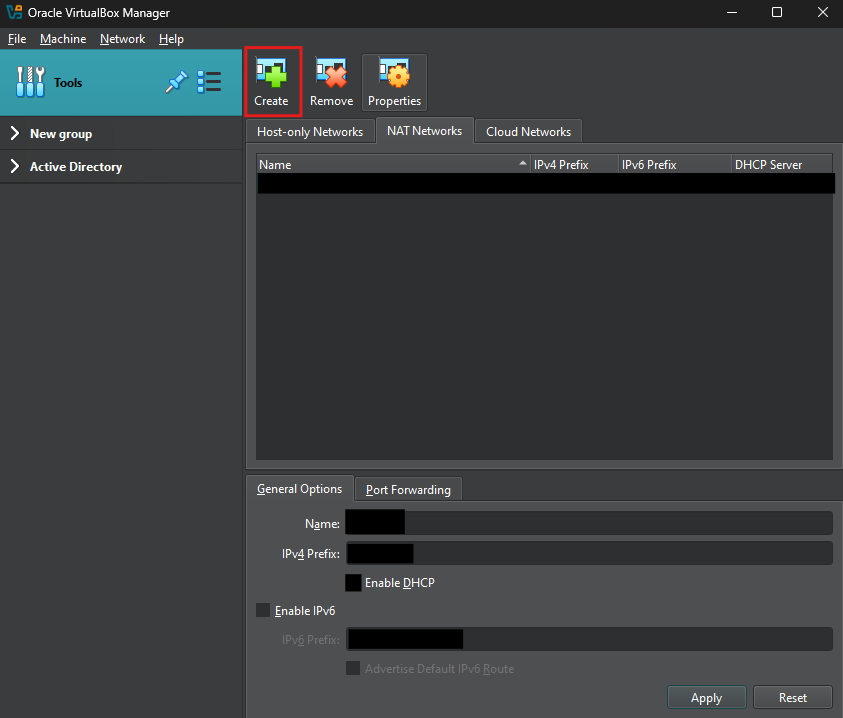
Once the command execution is completed, hit enter on the following screen.

Ubuntu server installation.

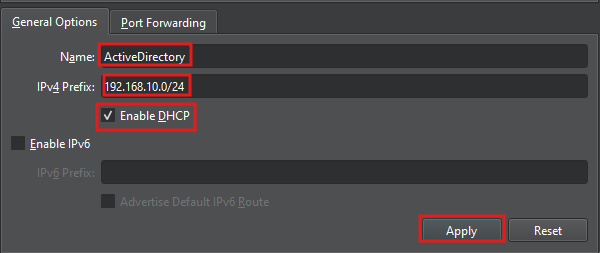
Now, the Ubuntu server VM is ready.

#### **5. Network Configuration**

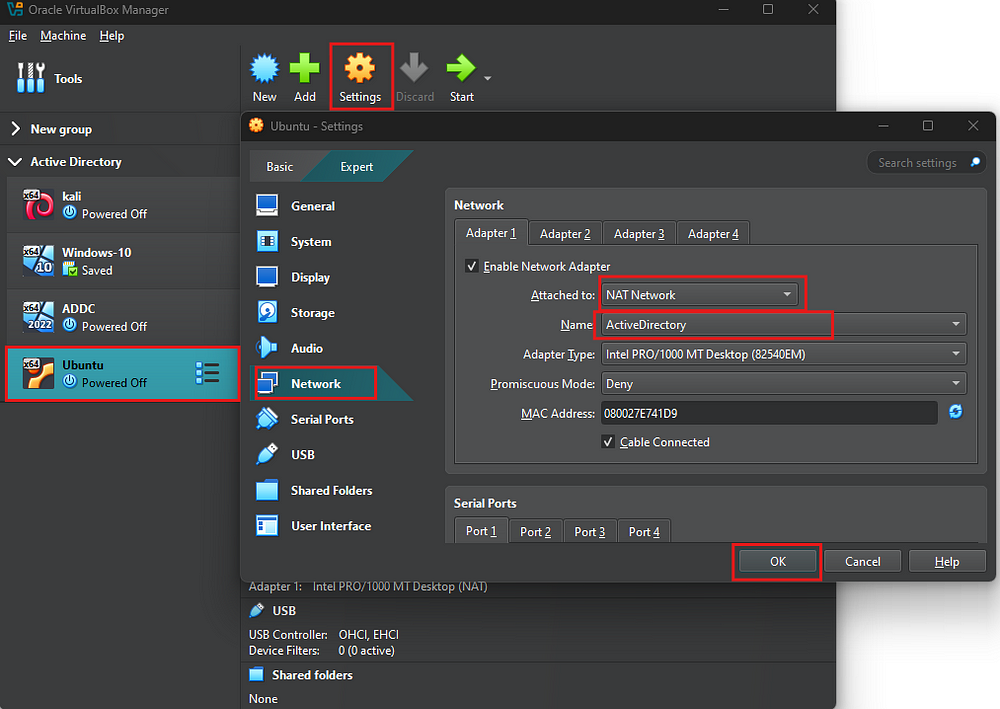
In the VirtualBox, click on tools and under the three dots select Network option. Under the network, select Nat Networks and click on create.

Network Configuration.

Under the General options enter the Name and IPv4 Prefix and check Enable DHCP and click apply.

Network Configuration.

Now select the Ubuntu VM, go to settings, go to Network and under this select the adapter to NAT Network and select the above created adapter and click ok.

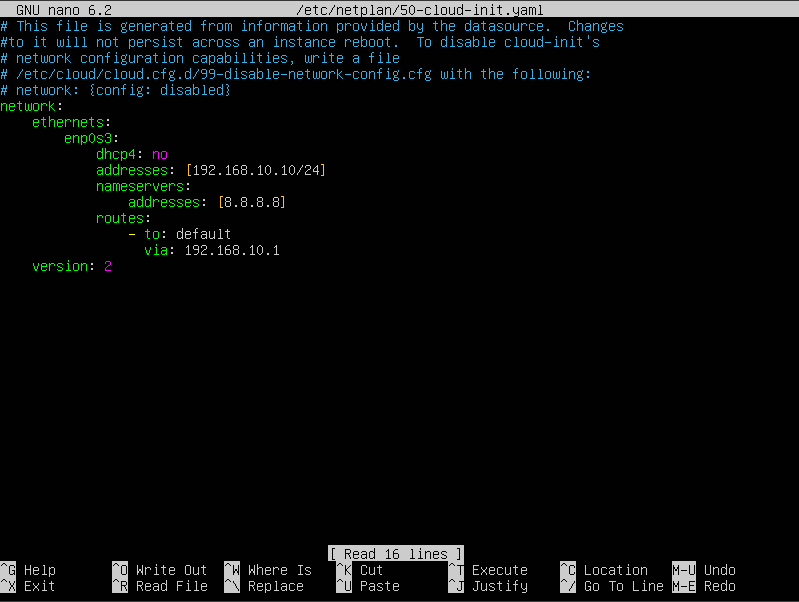
Network Configuration.

Repeat the same step for all the VM’s.

For the Ubuntu server eneter the following command and change the IP address to reflect our IP address.

sudo nano /etc/netplan/50-cloud-init.yaml

Now edit the file to reflect the following configuration.

Ubuntu Server static IP config.

This will set the Ubuntu server’s IP to a static IP which will reflect our initial network Diagram.

Now, we can Install Splunk Enterprise. Please go to Splunk Installation blog, to check Splunk installation and setup.

#### 