



**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**

P.O Bidholi, Via-Prem Nagar, Dehradun-248007

## **LAB REPORT**

# *Introduction to Virtualization And Cloud Computing [IVCC]*

Session-2021-22



**Submitted By:** Hitendra Sisodia

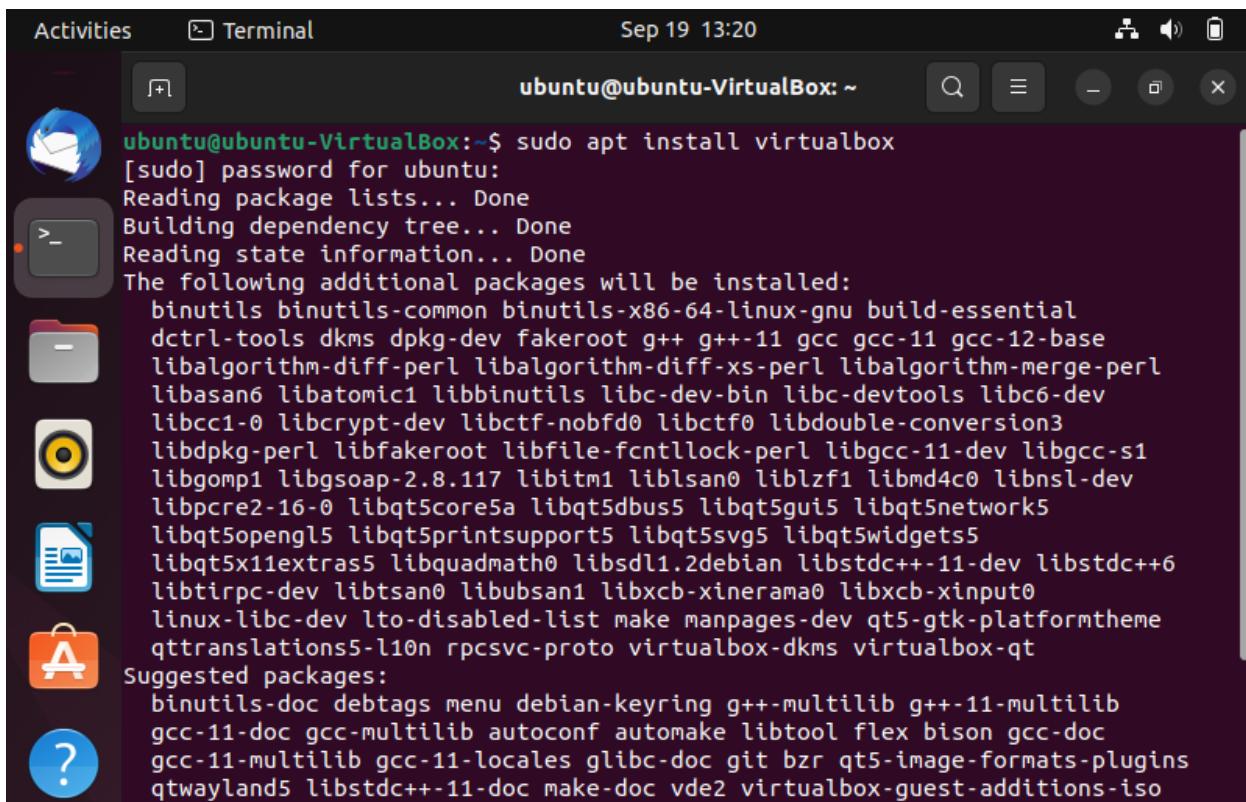
**Roll No:** R2142210352

**Sap Id:** 500091882

**Guided By:** Dr. Anurag Jain

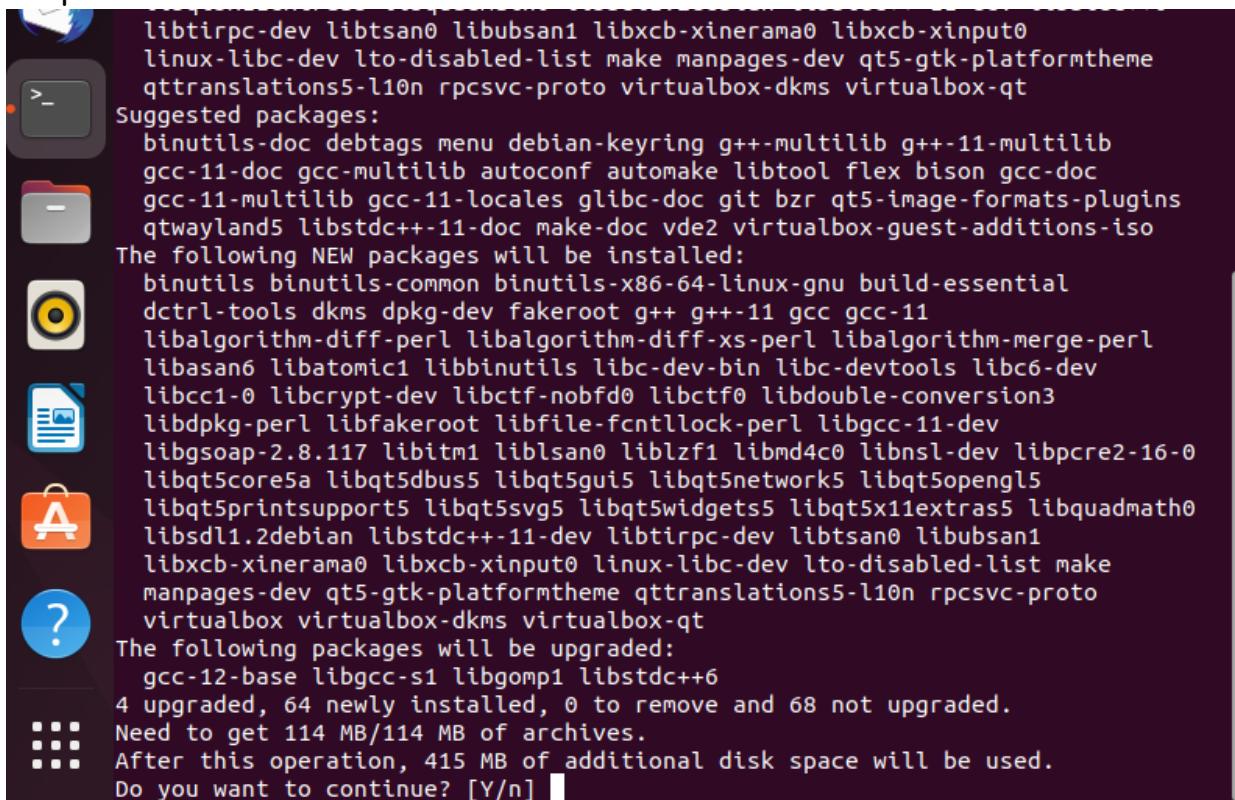
## Lab 6: Installing Virt-Manager And Installing VM

Step1: sudo apt install virtulabox: for installing virtualbox setup.



```
Activities Terminal Sep 19 13:20
ubuntu@ubuntu-VirtualBox:~$ sudo apt install virtualbox
[sudo] password for ubuntu:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
binutils binutils-common binutils-x86_64-linux-gnu build-essential
dctrl-tools dkms dpkg-dev fakeroot g++ g++-11 gcc gcc-11 gcc-12-base
libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl
libasan6 libatomic1 libbinutils libc-dev-bin libc-devtools libc6-dev
libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libdouble-conversion3
libdpkg-perl libfakeroot libfile-fcntllock-perl libgcc-11-dev libgcc-s1
libgomp1 libgsoap-2.8.117 libitm1 liblsan0 liblzf1 libmd4c0 libnsl-dev
libpcre2-16-0 libqt5core5a libqt5dbus5 libqt5gui5 libqt5network5
libqt5opengl5 libqt5printsupport5 libqt5svg5 libqt5widgets5
libqt5x11extras5 libquadmath0 libsdl1.2debian libstdc++-11-dev libstdc+++
libtirpc-dev libtsan0 libubsan1 libxcb-xinerama0 libxcb-xinput0
linux-libc-dev lto-disabled-list make manpages-dev qt5-gtk-platformtheme
qttranslations5-l10n rpcsvc-proto virtualbox-dkms virtualbox-qt
Suggested packages:
binutils-doc debtags menu debian-keyring g++-multilib g++-11-multilib
gcc-11-doc gcc-multilib autoconf automake libtool flex bison gcc-doc
gcc-11-multilib gcc-11-locales glibc-doc git bzr qt5-image-formats-plugins
qtwayland5 libstdc++-11-doc make-doc vde2 virtualbox-guest-additions-iso
```

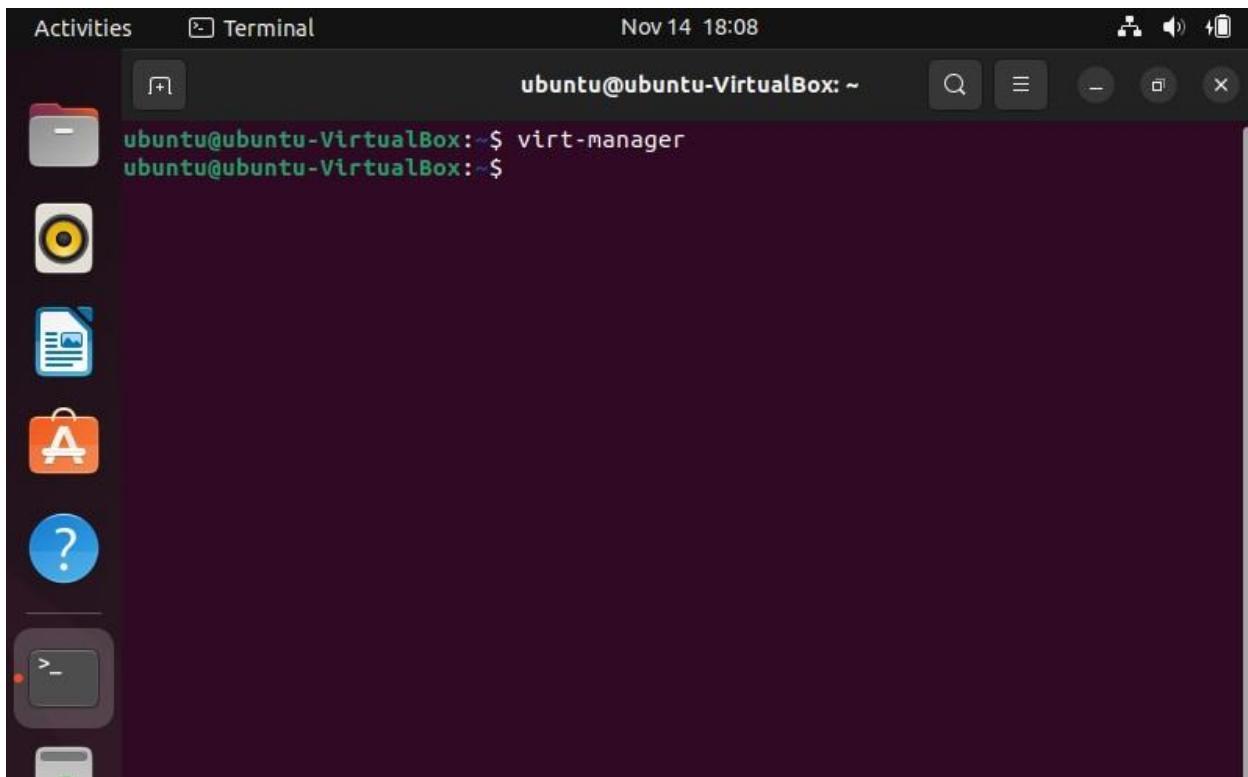
Step2: Press Y for continue.



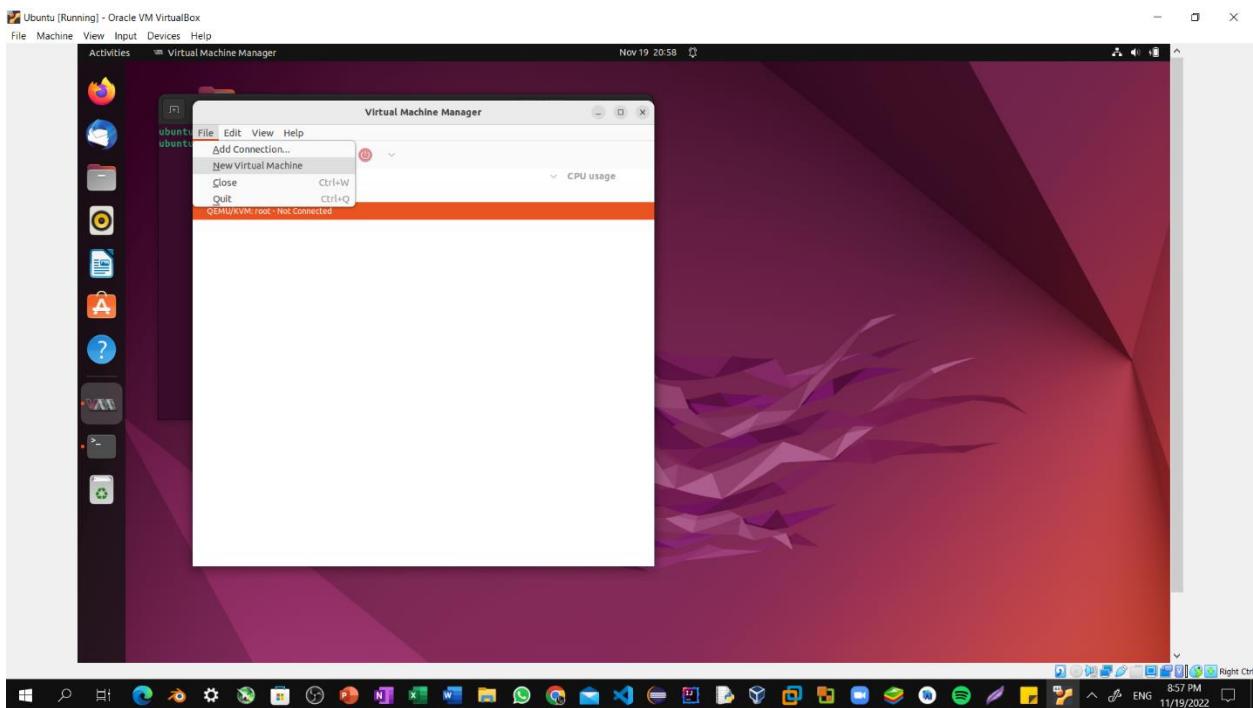
```
libtirpc-dev libtsan0 libubsan1 libxcb-xinerama0 libxcb-xinput0
linux-libc-dev lto-disabled-list make manpages-dev qt5-gtk-platformtheme
qttranslations5-l10n rpcsvc-proto virtualbox-dkms virtualbox-qt
Suggested packages:
binutils-doc debtags menu debian-keyring g++-multilib g++-11-multilib
gcc-11-doc gcc-multilib autoconf automake libtool flex bison gcc-doc
gcc-11-multilib gcc-11-locales glibc-doc git bzr qt5-image-formats-plugins
qtwayland5 libstdc++-11-doc make-doc vde2 virtualbox-guest-additions-iso
The following NEW packages will be installed:
binutils binutils-common binutils-x86_64-linux-gnu build-essential
dctrl-tools dkms dpkg-dev fakeroot g++ g++-11 gcc gcc-11
libalgorithm-diff-perl libalgorithm-diff-xs-perl libalgorithm-merge-perl
libasan6 libatomic1 libbinutils libc-dev-bin libc-devtools libc6-dev
libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libdouble-conversion3
libdpkg-perl libfakeroot libfile-fcntllock-perl libgcc-11-dev
libgsoap-2.8.117 libitm1 liblsan0 liblzf1 libmd4c0 libnsl-dev libpcre2-16-0
libqt5core5a libqt5dbus5 libqt5gui5 libqt5network5 libqt5opengl5
libqt5printsupport5 libqt5svg5 libqt5widgets5 libqt5x11extras5 libquadmath0
libsdl1.2debian libstdc++-11-dev libtirpc-dev libtsan0 libubsan1
libxcb-xinerama0 libxcb-xinput0 linux-libc-dev lto-disabled-list make
manpages-dev qt5-gtk-platformtheme qttranslations5-l10n rpcsvc-proto
virtualbox virtualbox-dkms virtualbox-qt
The following packages will be upgraded:
gcc-12-base libgcc-s1 libgomp1 libstdc+++
4 upgraded, 64 newly installed, 0 to remove and 68 not upgraded.
Need to get 114 MB/114 MB of archives.
After this operation, 415 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

## Lab 6: Installing Virt-Manager And Installing VM

Step3: virt-manager: for launching QEMU Interface form terminal.

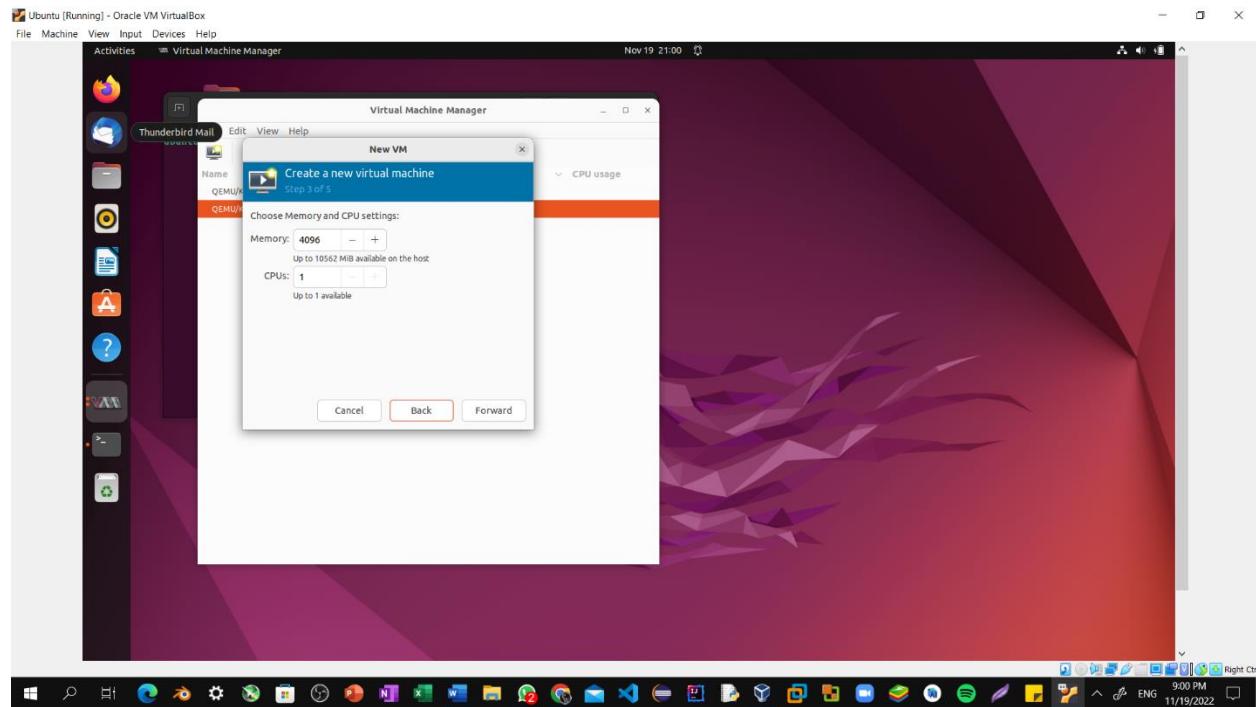


Step4: Click on New Button and Select name of Virtual Operating System i.e., Windows 7.

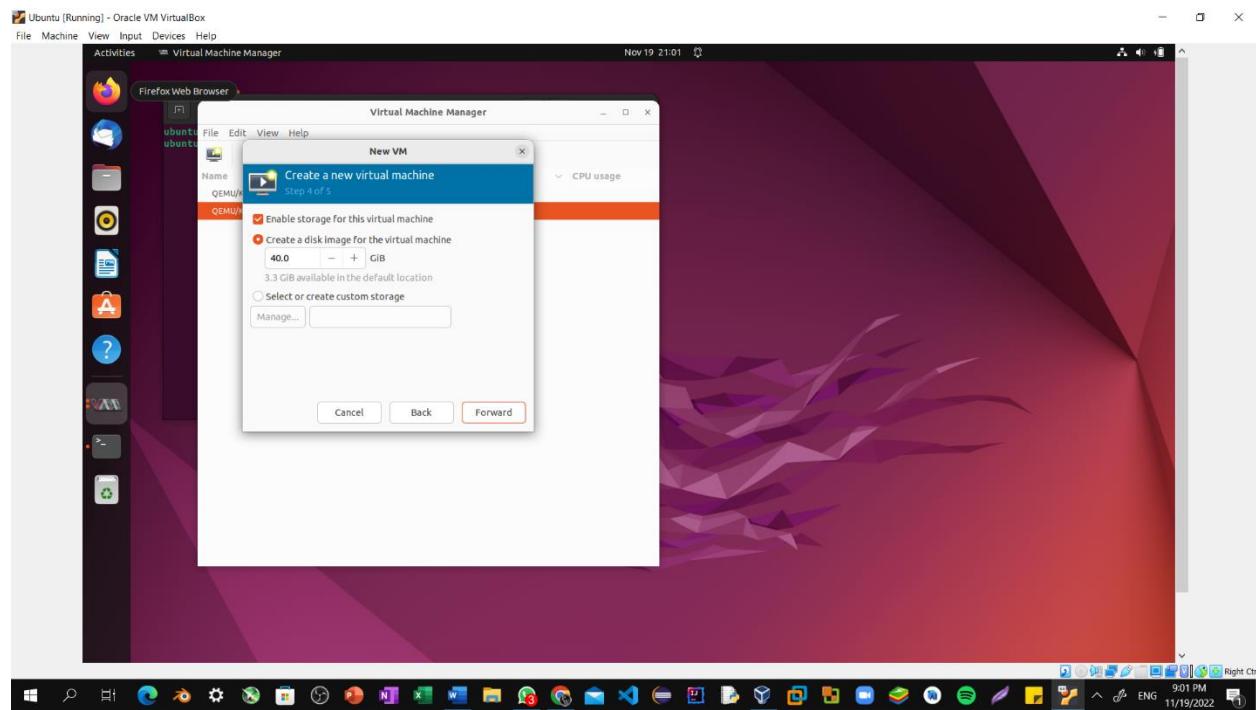


## Lab 6: Installing Virt-Manager And Installing VM

Step5: Now Select Memory Size depending upon the Usability.

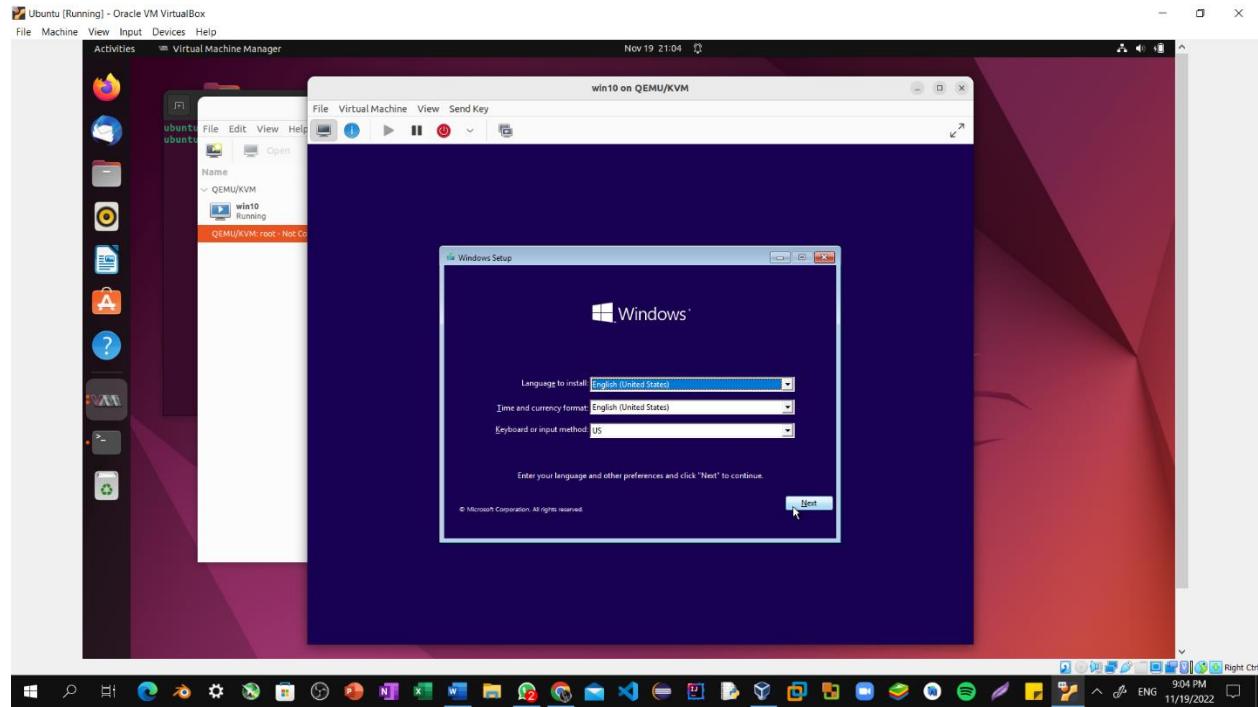


Step6: Select create a Virtual Hard Disk and click next.

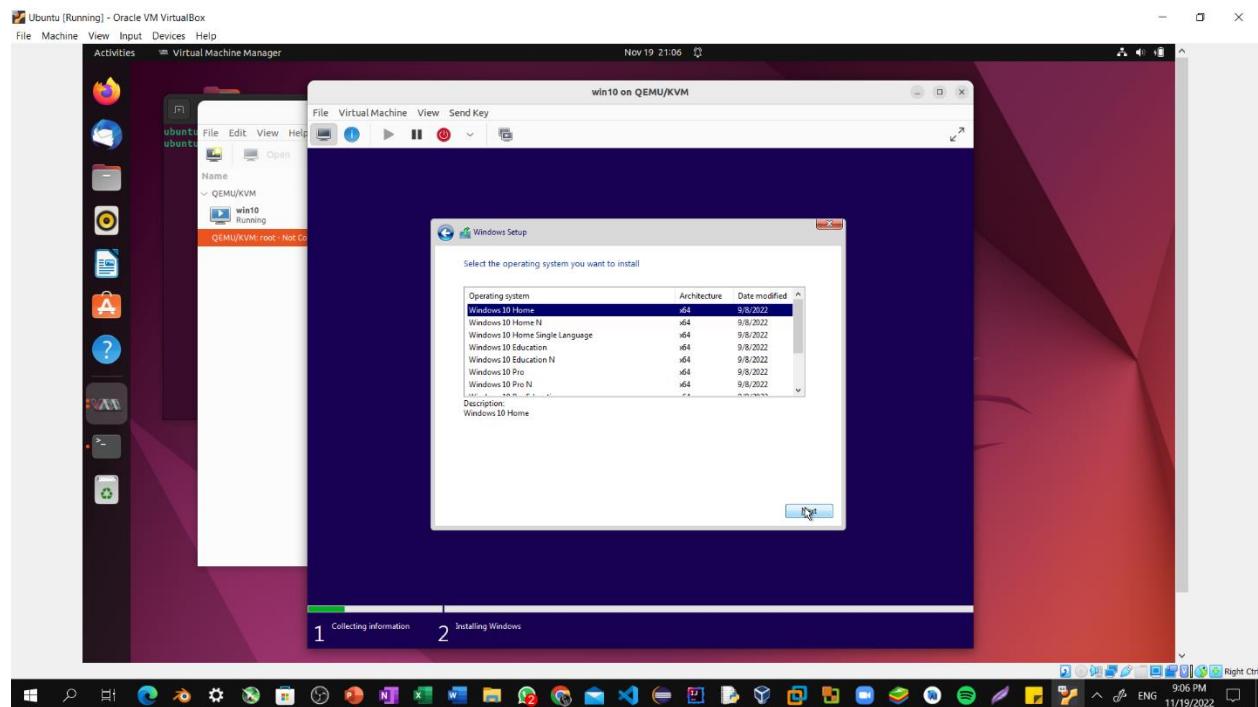


## Lab 6: Installing Virt-Manager And Installing VM

Step7: Then Select Install Windows10 and then on next.

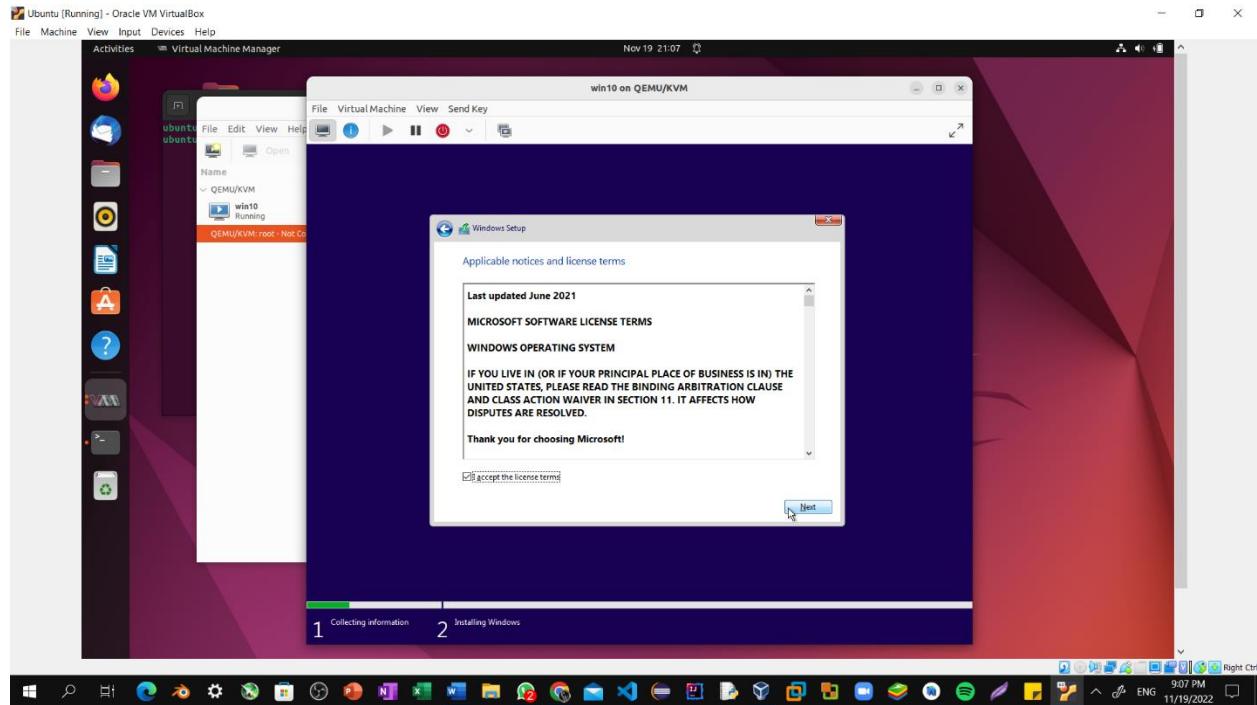


Step8: Select Windows 10 Home and proceed further by clicking on next.

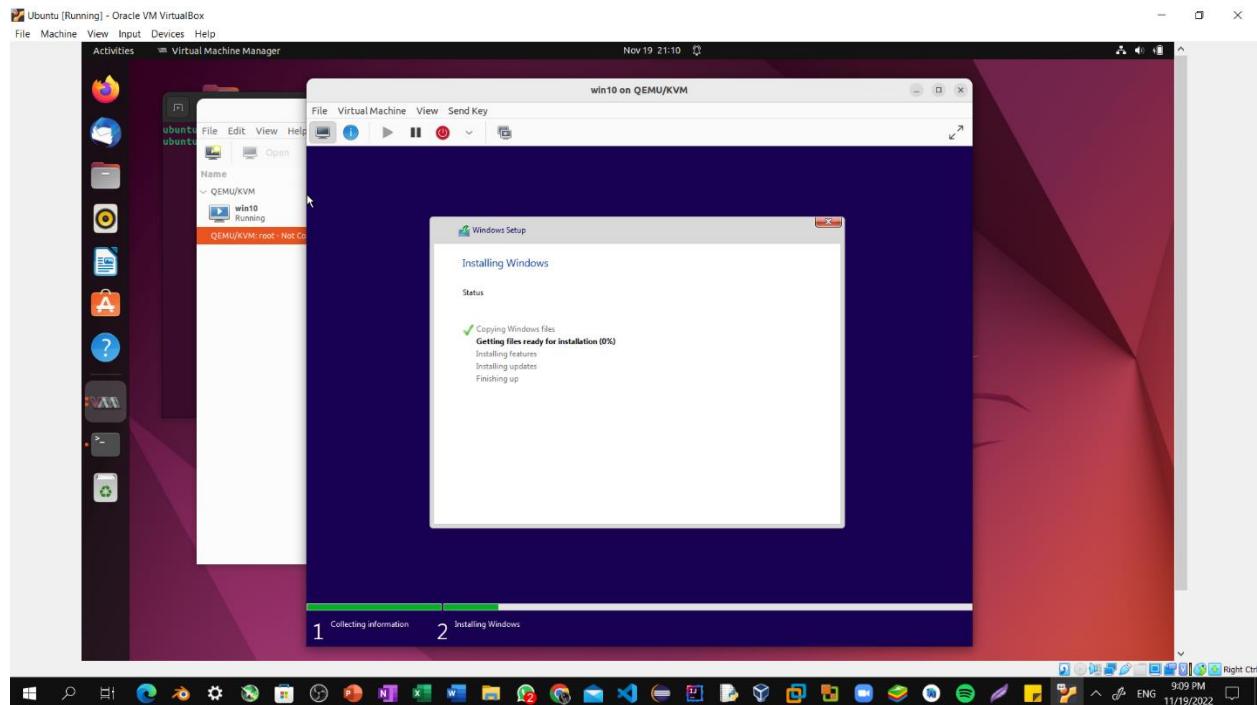


## Lab 6: Installing Virt-Manager And Installing VM

Step9: Check I accept the license terms and click on next.

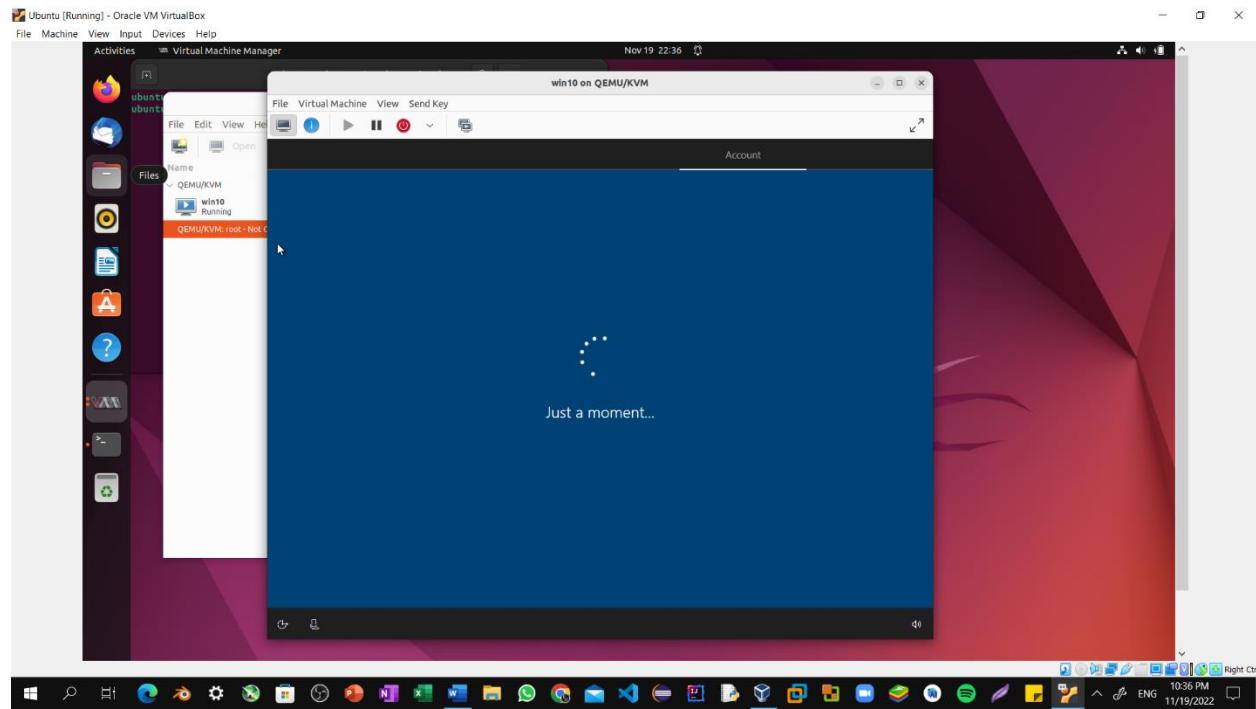


Step10: Getting Files ready for installation.

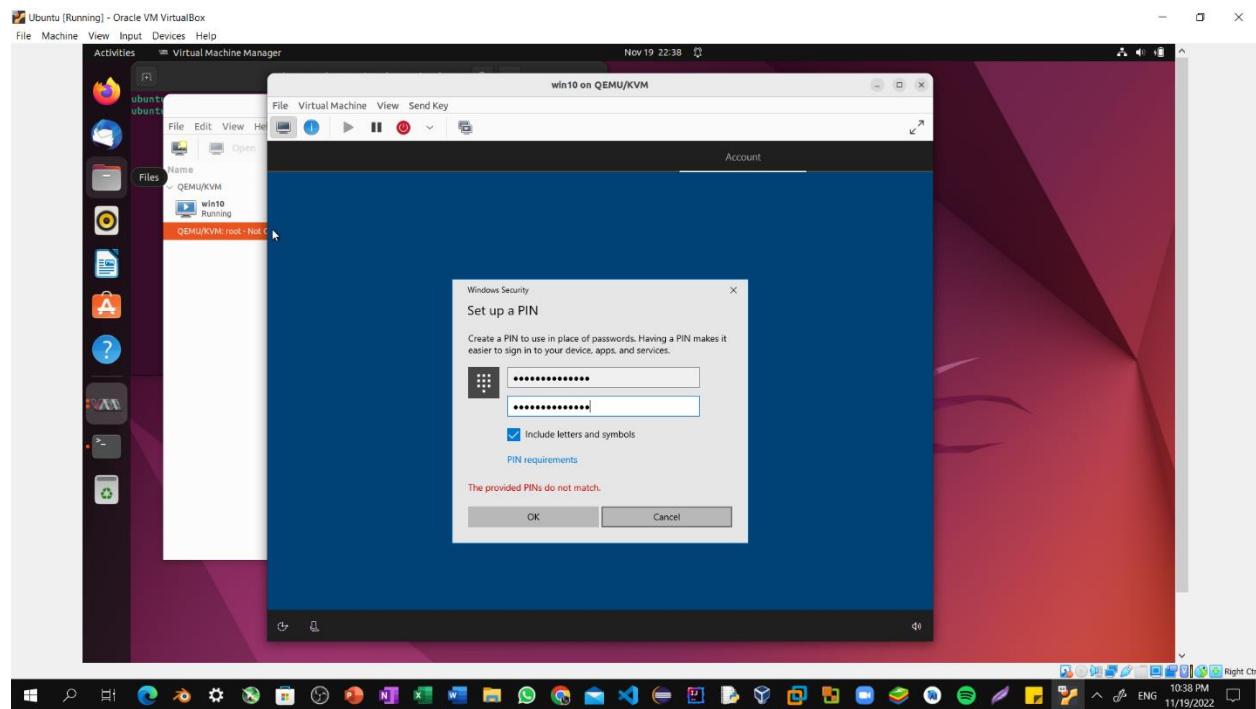


## Lab 6: Installing Virt-Manager And Installing VM

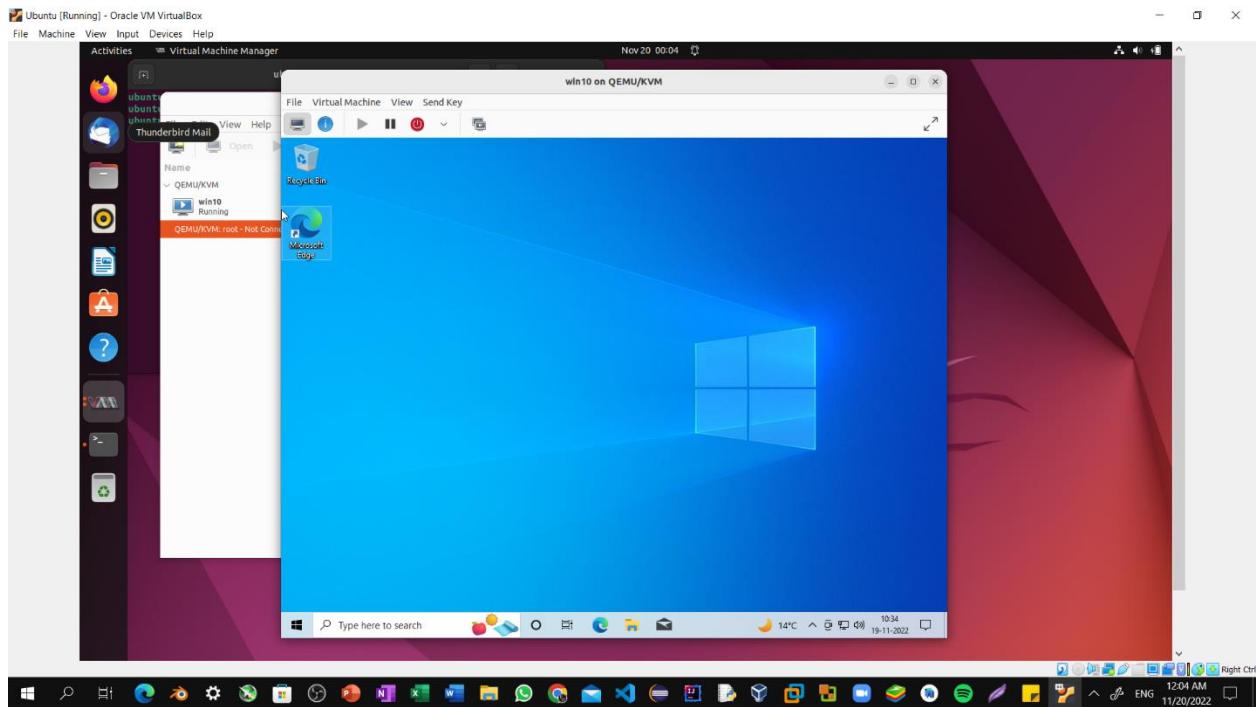
Step10: Wait For installation.



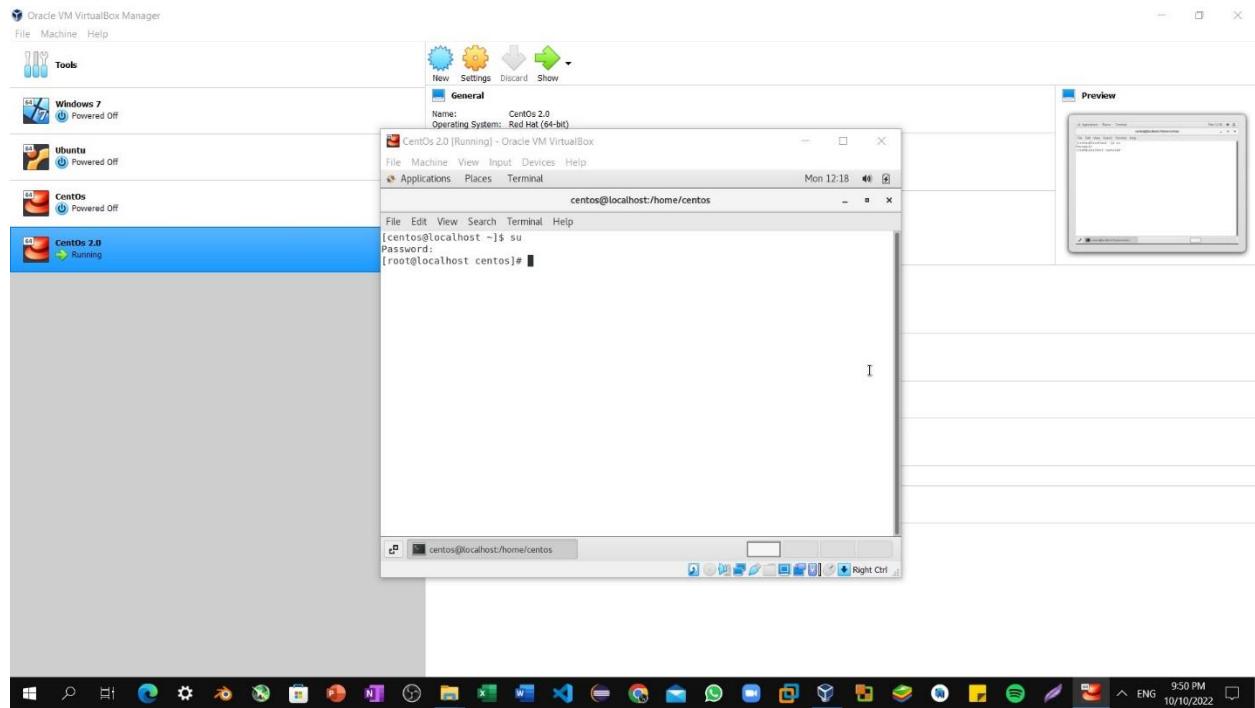
Step11: Setup pin for Windows workspace.



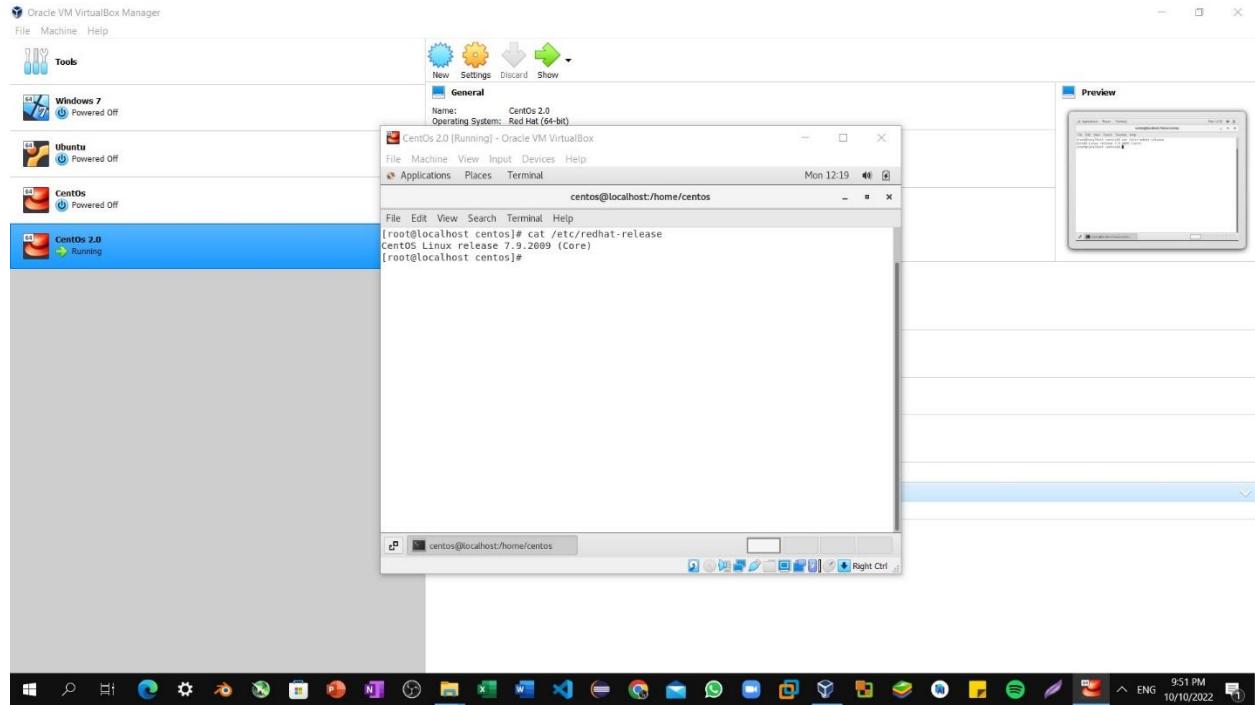
### Step12: Windows 10 Workspace.



### Step1: Enter in the root mode using su command

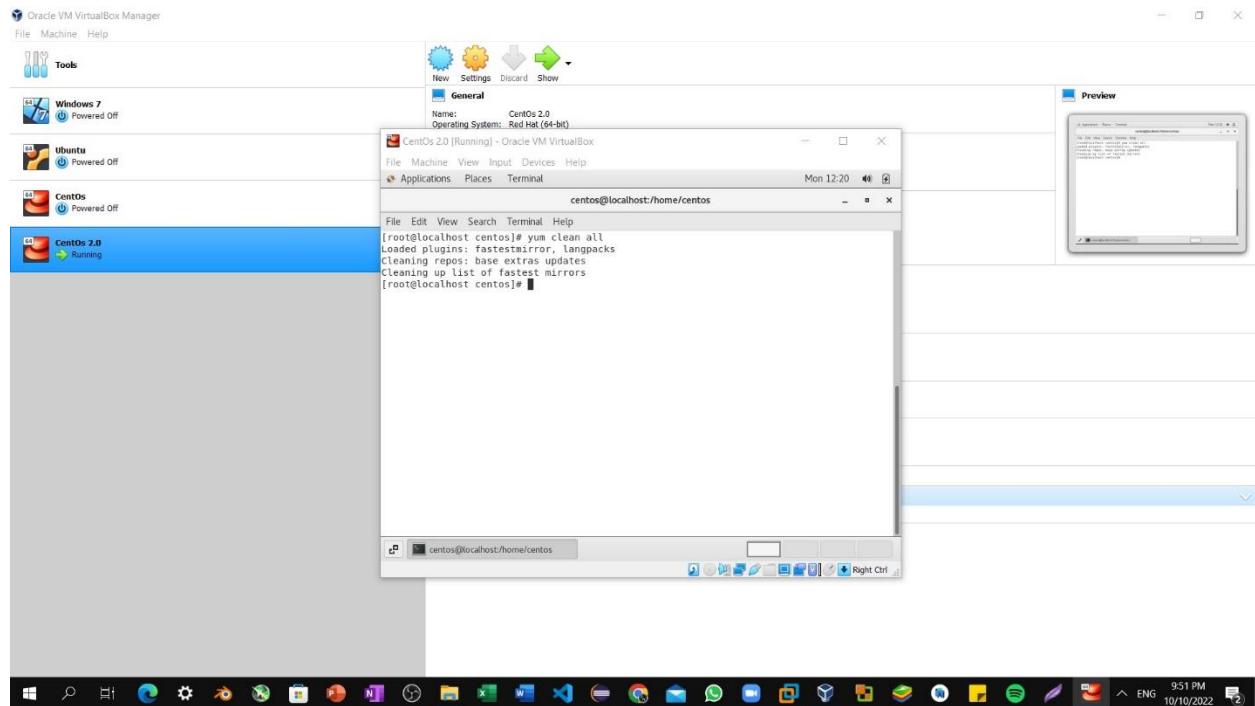


### Step2: cat /etc/redhat-release: Enter the following Linux command to display the current operating system information and its version.

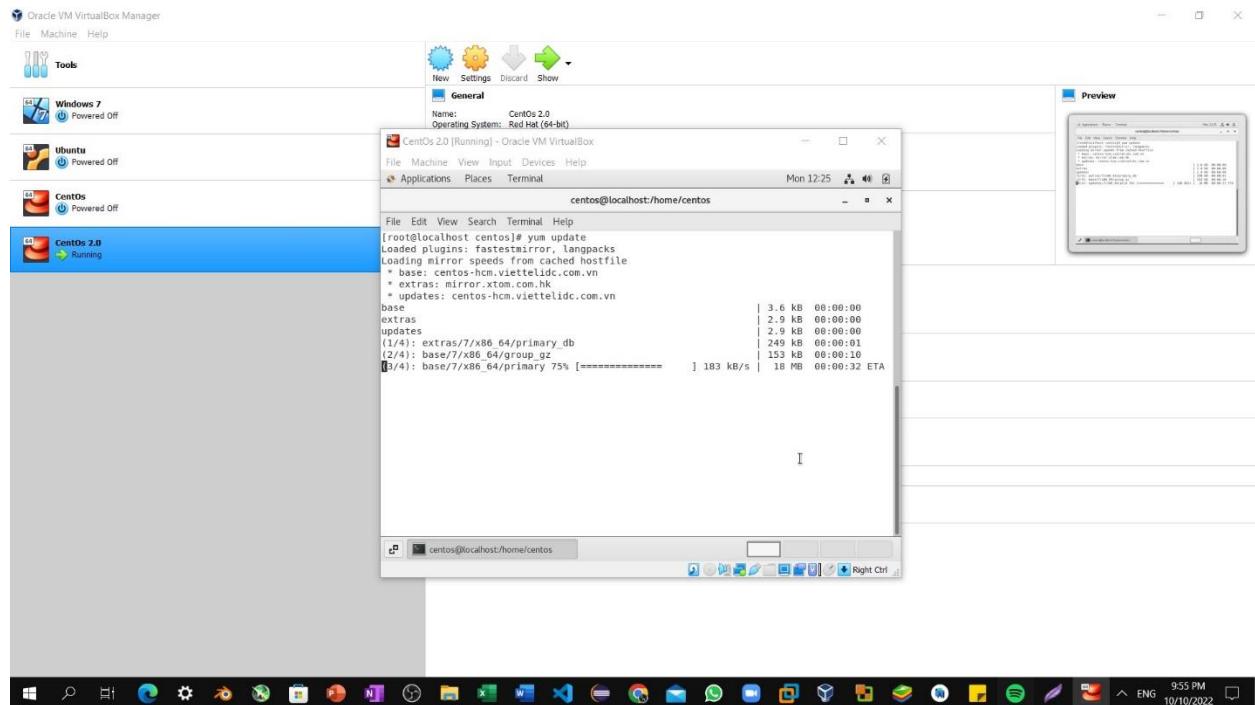


## Lab 7: Installing QEMU & KVM Through Commands

**Step3: yum clean all:** Enter the following commands in order for the operating system to be cleaned and updated.

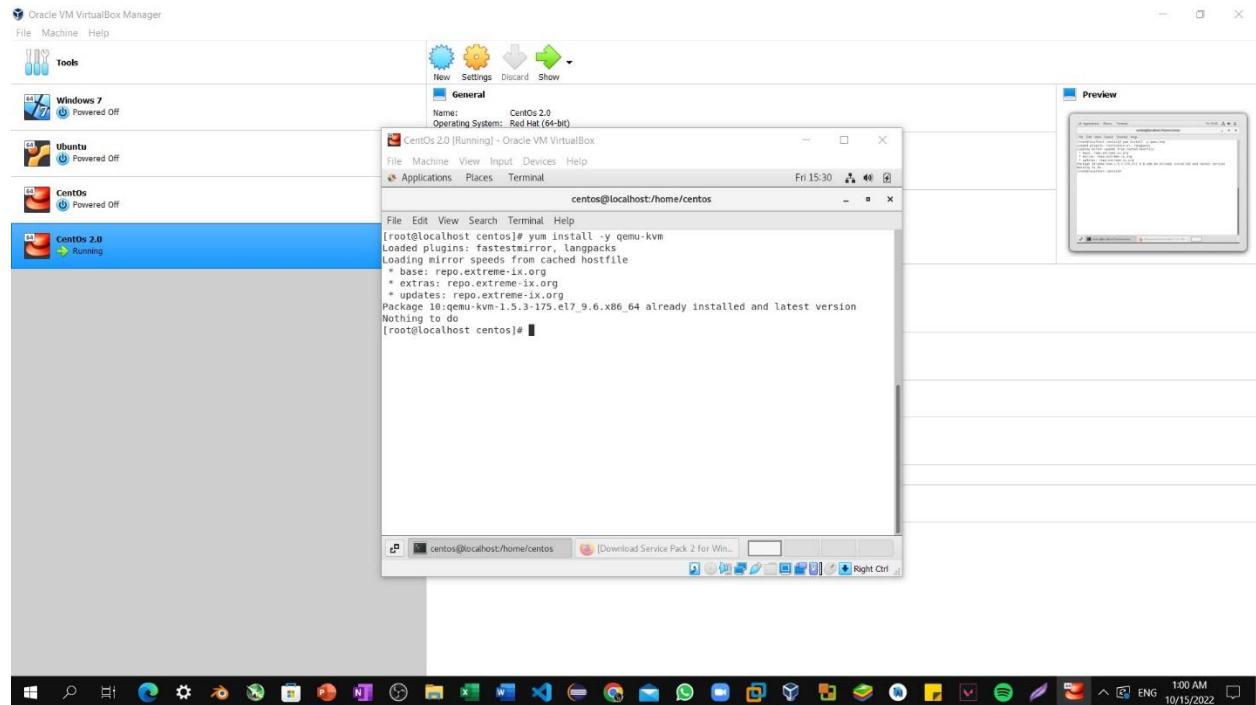


**Step4: yum update:** Enter the following commands in order for the operating system to be cleaned and updated. Then reboot your system.

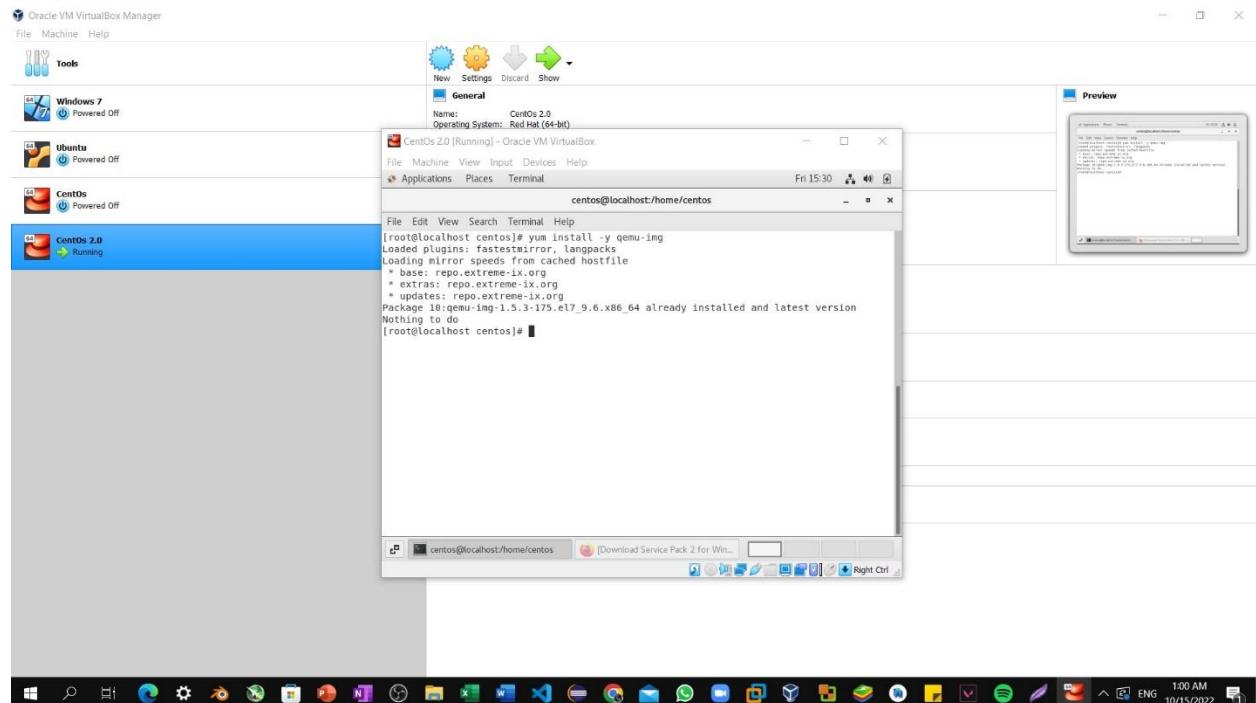


## Lab 7: Installing QEMU & KVM Through Commands

**Step5:** `yum install -y qemu-kvm`: This package provides the user-level KVM emulator and facilitates communication between hosts and guest virtual machines.

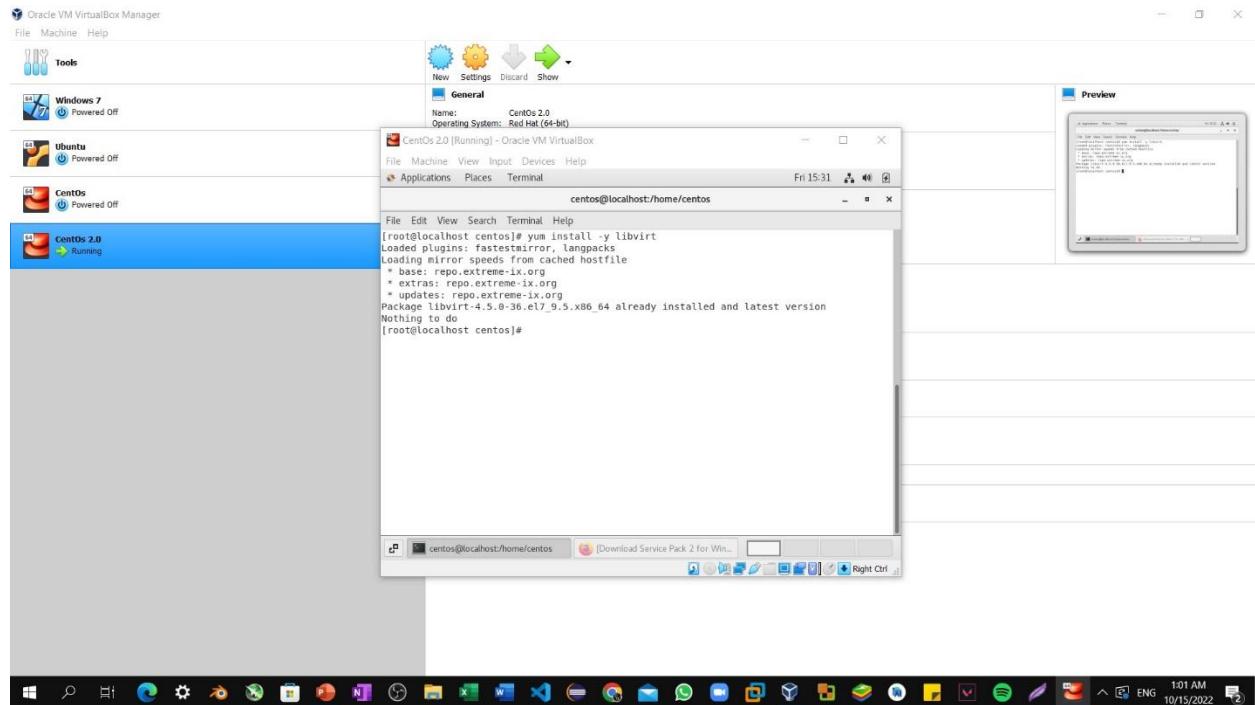


**Step6:** `yum install -y qemu-img`: This package provides disk management for guest virtual machines. The `qemu-img` package is installed as a dependency of the `qemu-kvm` package.

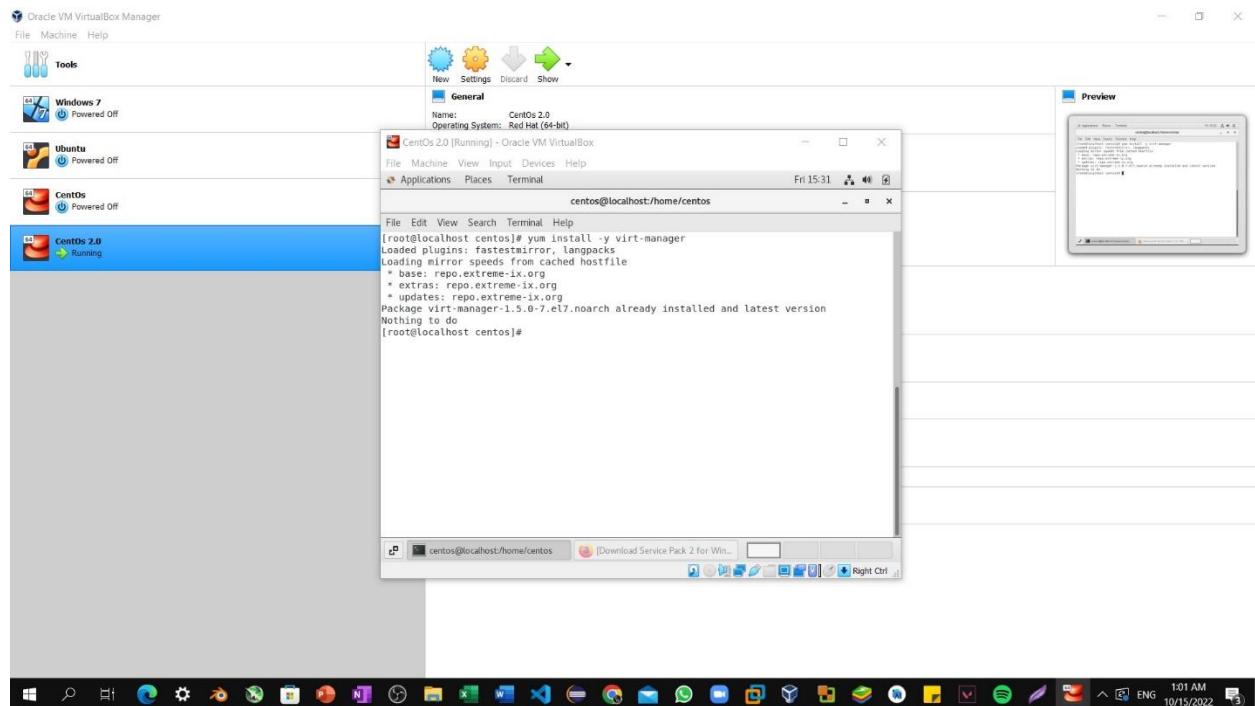


## Lab 7: Installing QEMU & KVM Through Commands

**Step7:** yum install -y libvirt: This package provides the server and host-side libraries for interacting with hypervisors and host systems.

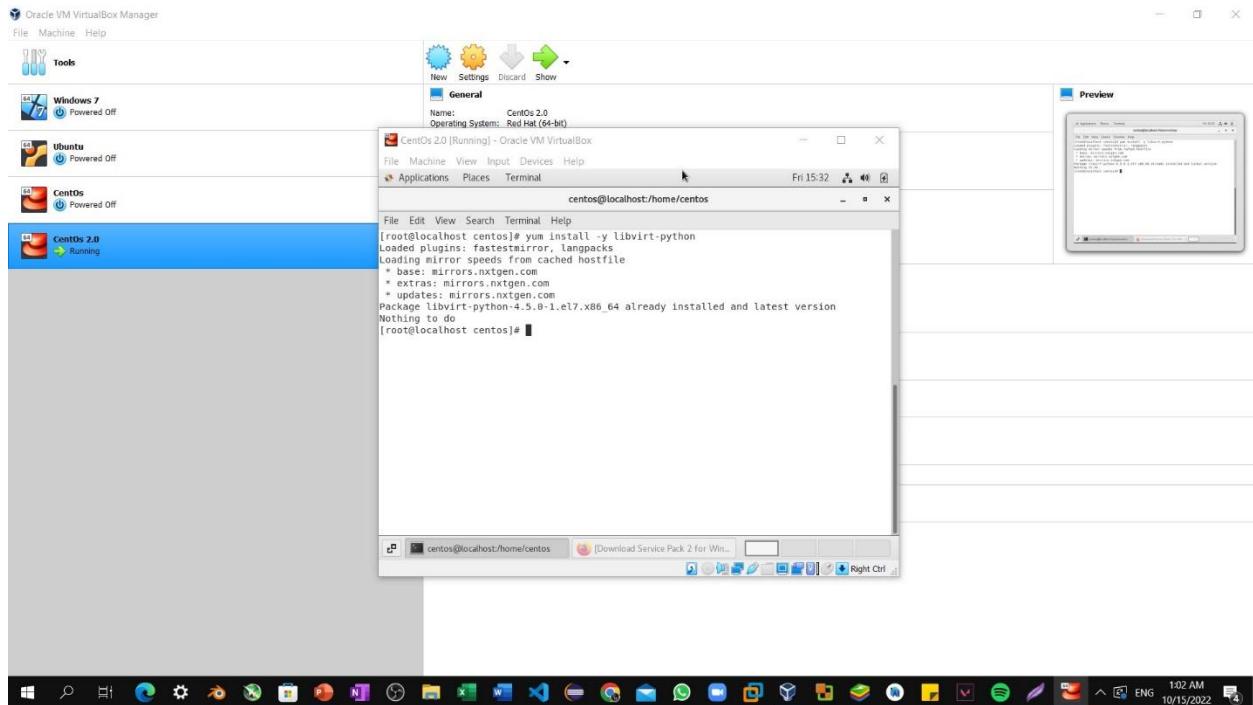


**Step8:** yum install -y virt-manager: This package provides the virt-manager tool, also known as Virtual Machine Manager.

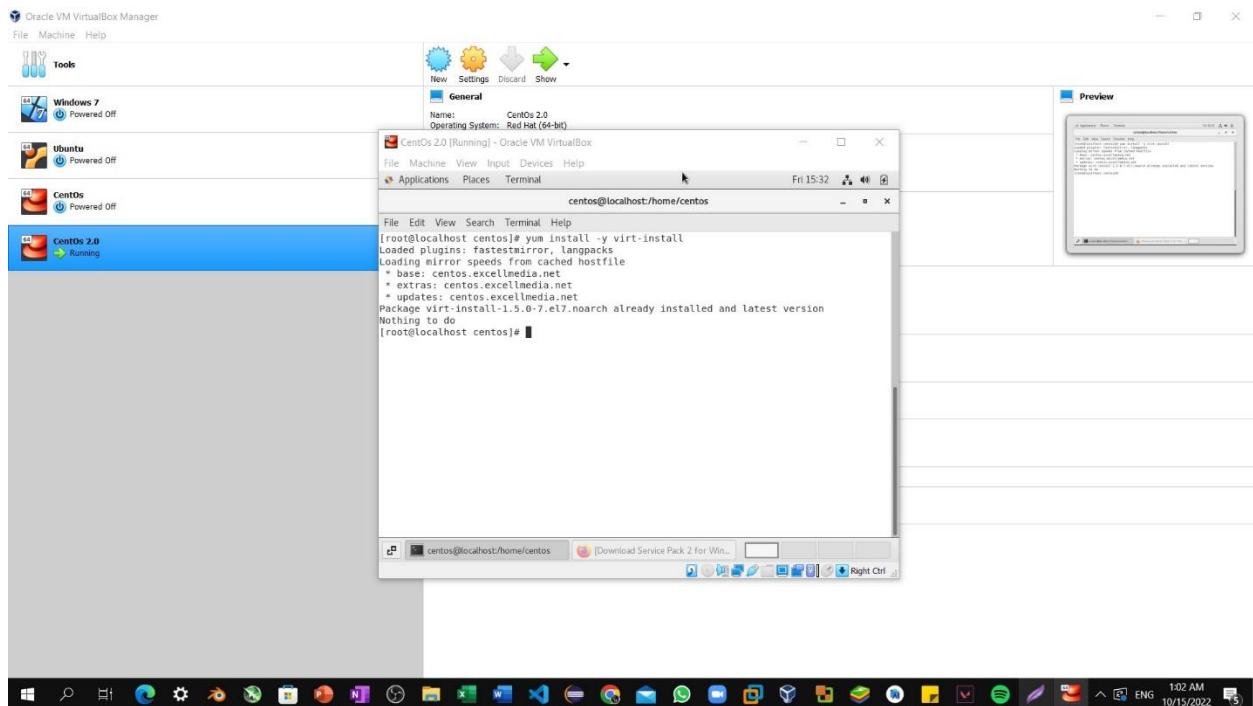


## Lab 7: Installing QEMU & KVM Through Commands

**Step9:** `yum install -y libvirt-python`: This package contains a module that permits applications written in the Python programming language to use the interface.

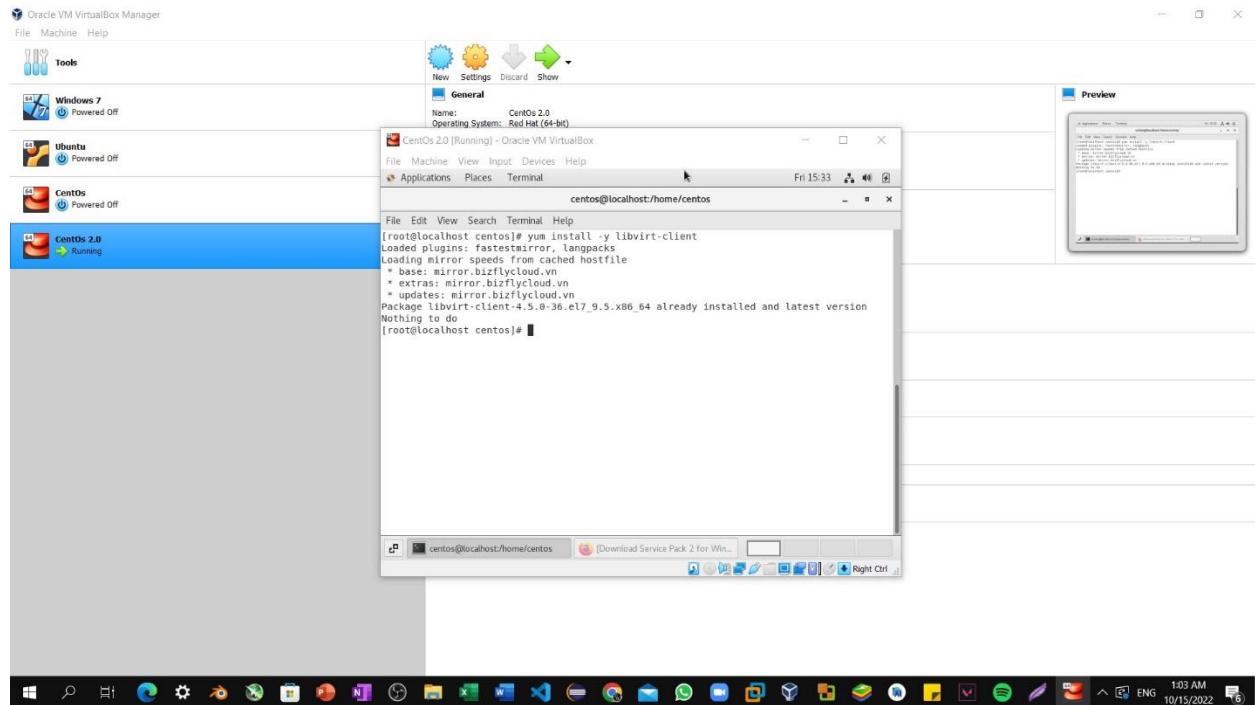


**Step10:** `yum install -y virt-install`: This package provides the `virt-install` command for creating virtual machines from the command line.

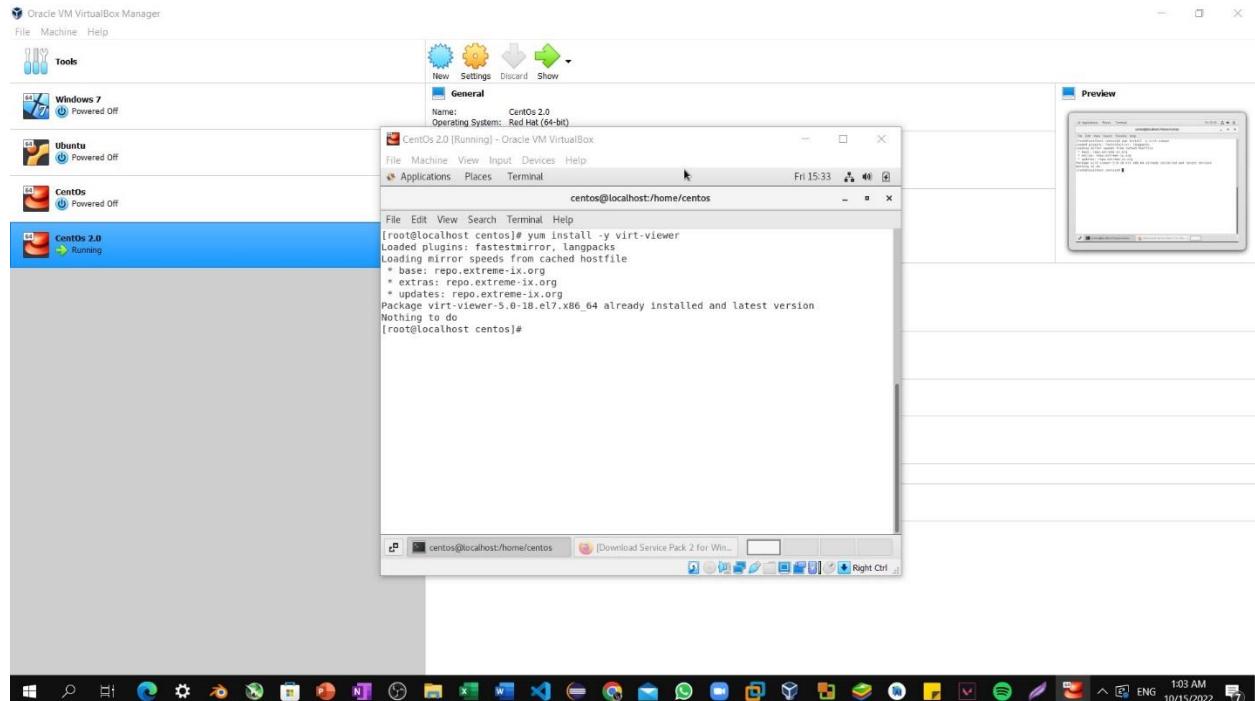


## Lab 7: Installing QEMU & KVM Through Commands

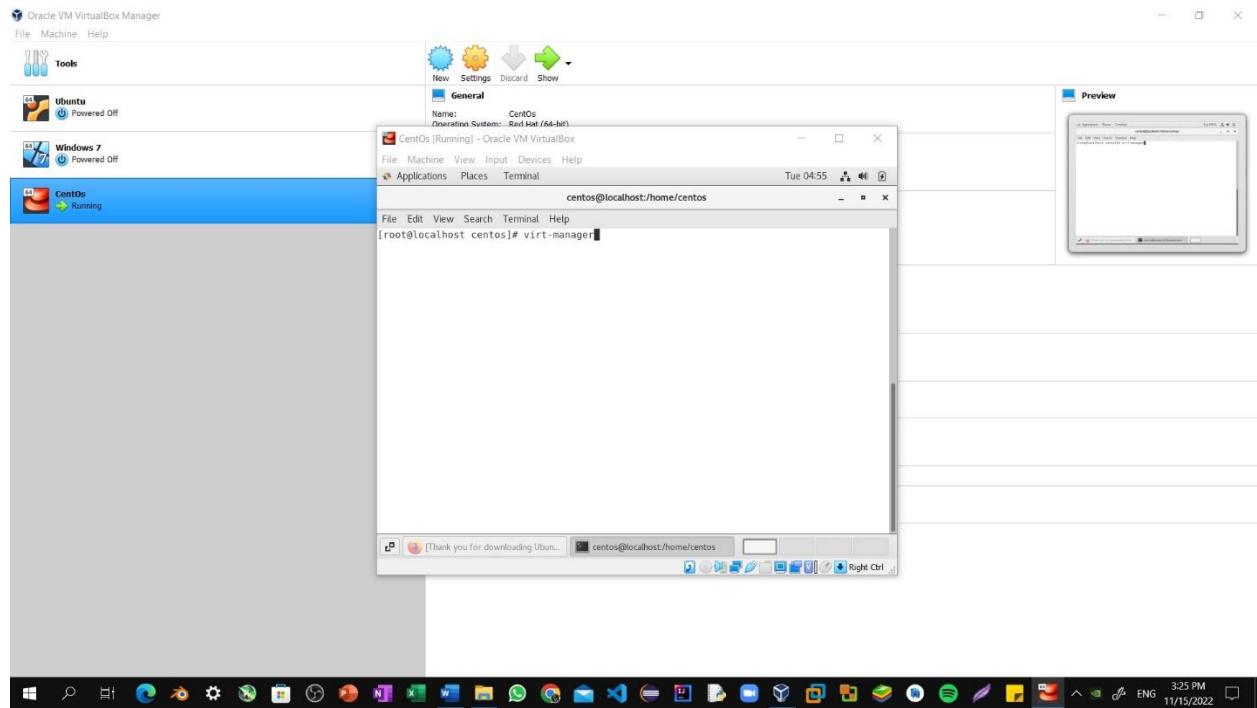
Step11: `yum install -y libvirt-client`: This package provides the client-side APIs and libraries for accessing libvirt servers.



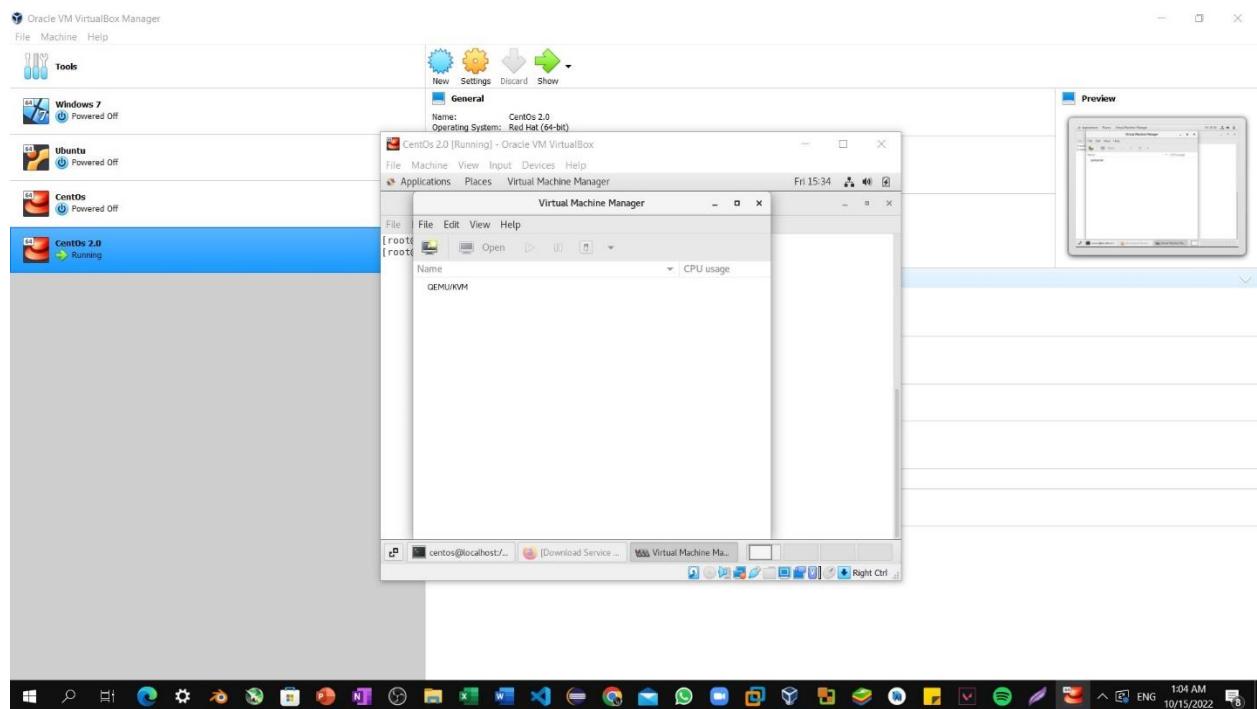
Step12: `yum install -y virt-viewer`: The virt-viewer package is designed for, Virtual Machine Viewer. Virtual Machine Viewer provides a graphical console client for connecting to virtual machines.



### Step13: virt-manager: Opening KVM Interface.

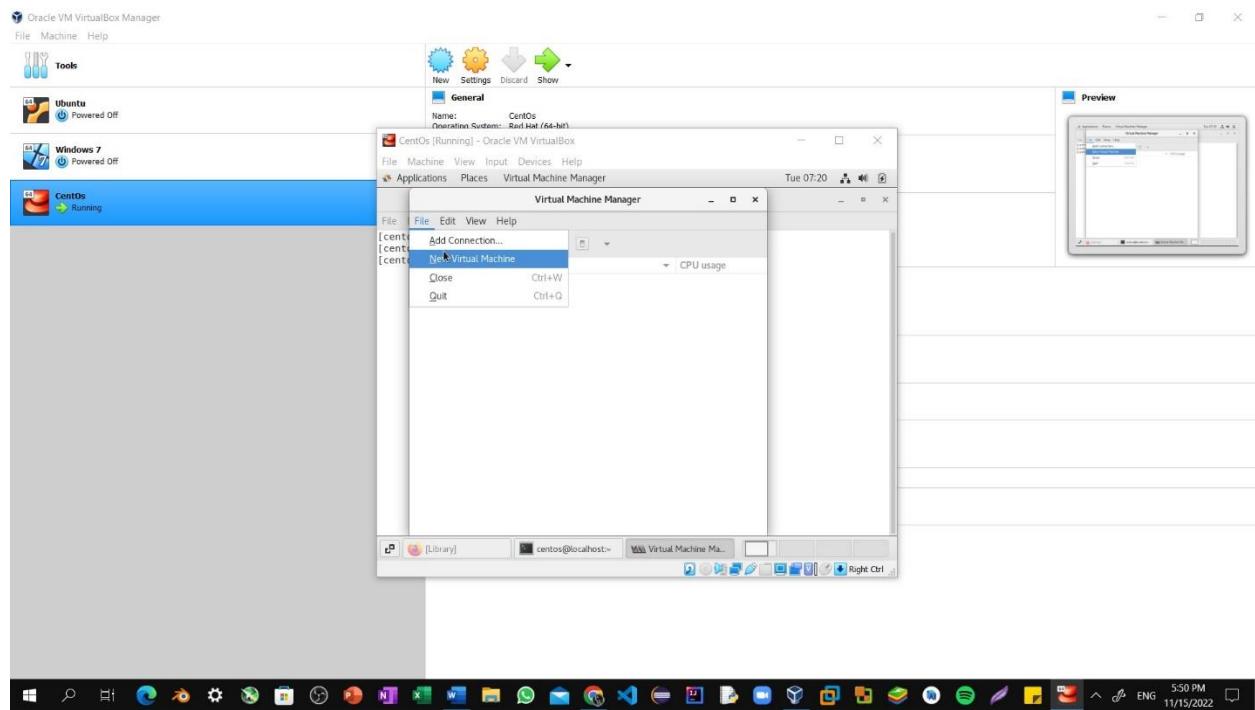


### Step14: KVM Interface

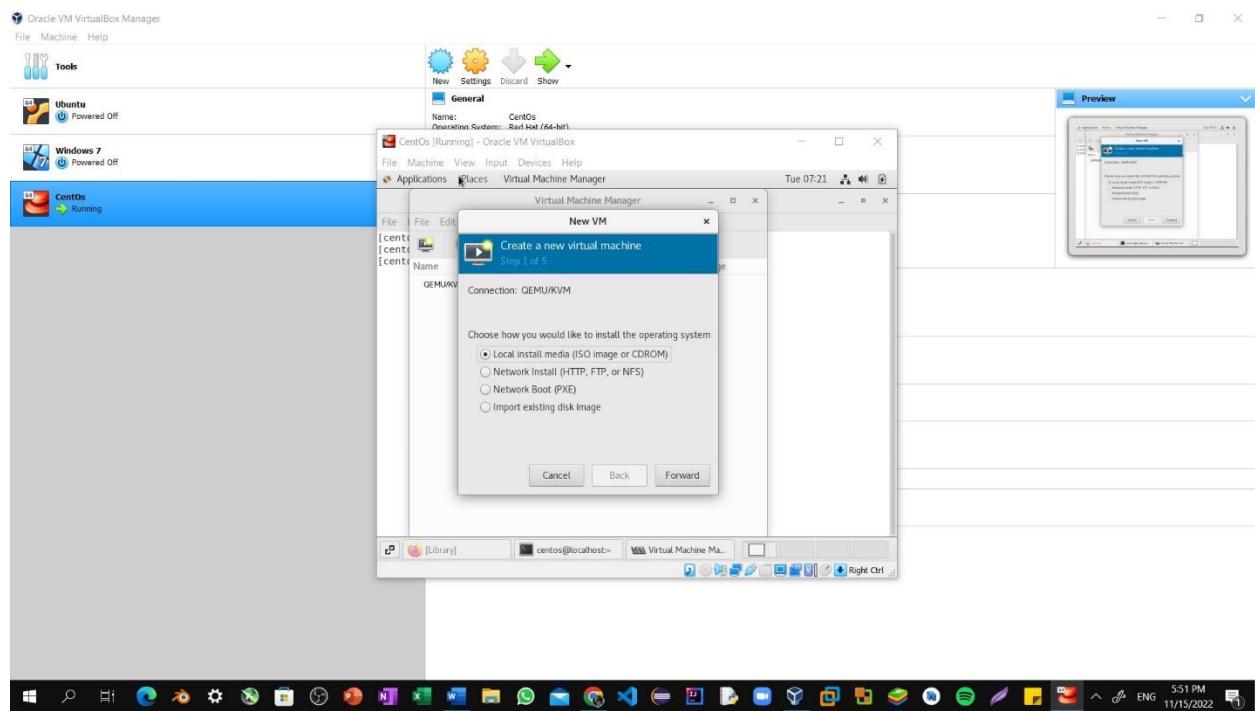


## Lab 8: Installing Ubuntu Within VM Using QEMU

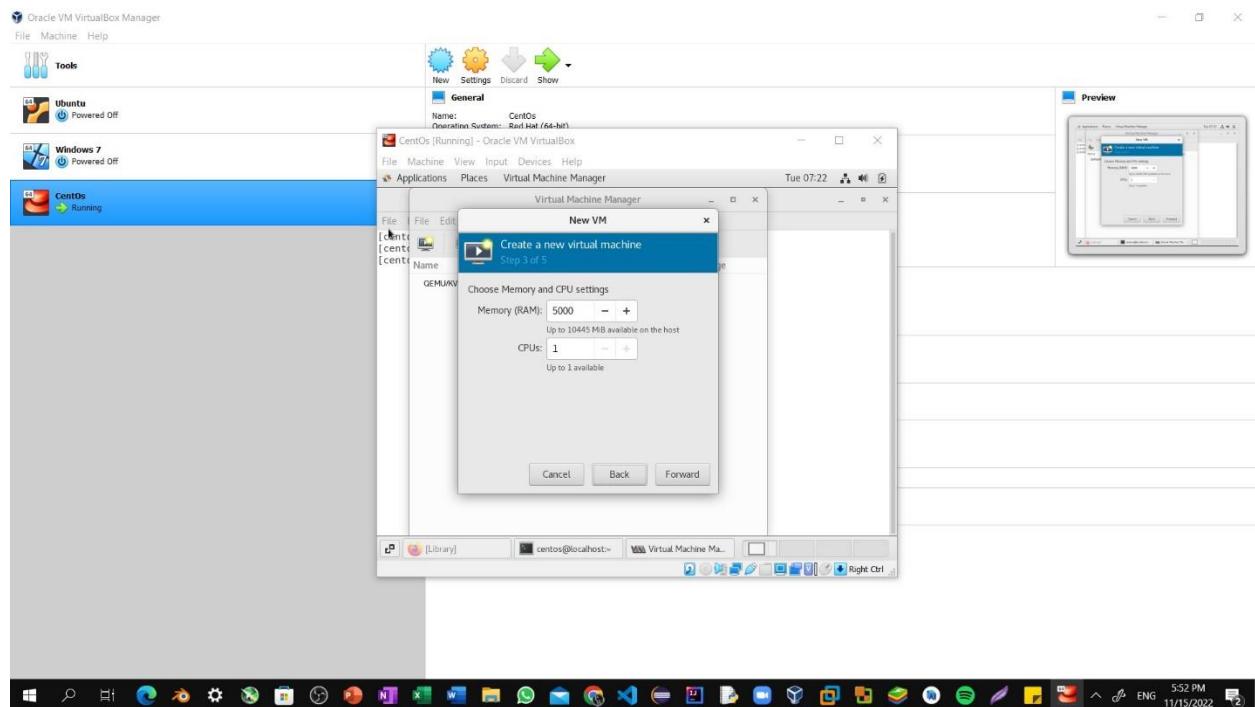
Step1: Go to file section, and click on New Virtual Machine.



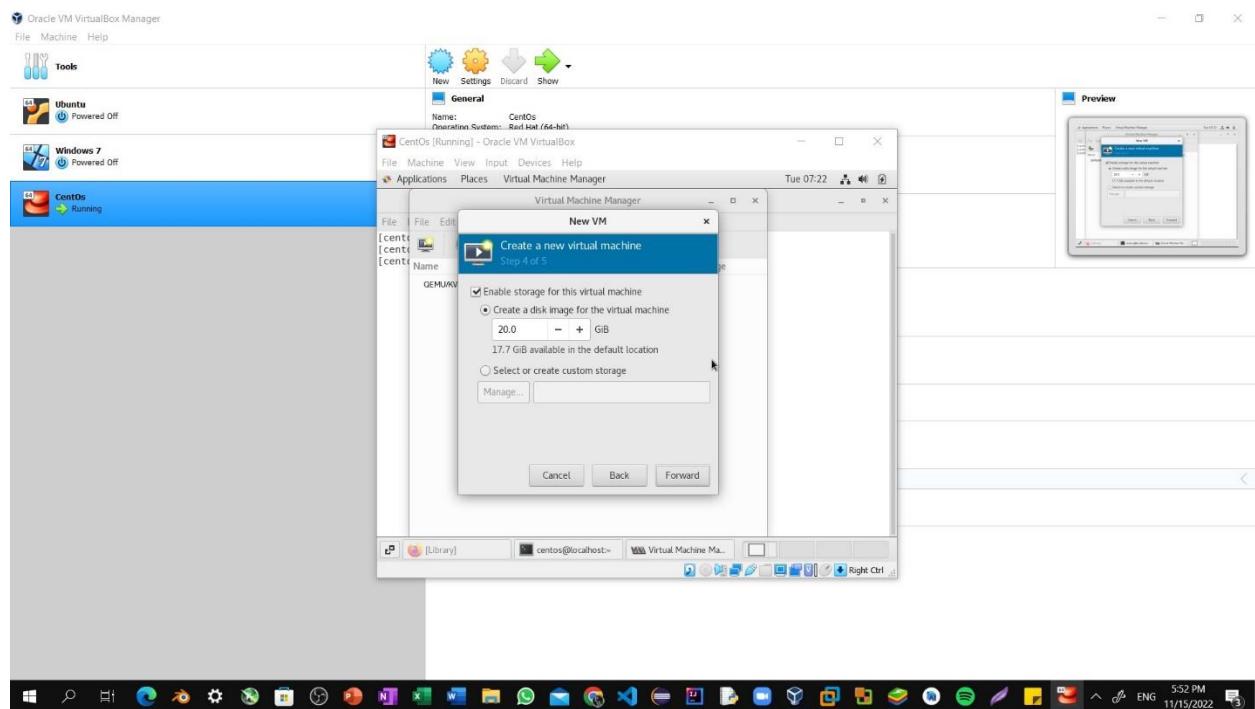
Step2: Remain Default Setting as it is and click on forward.



Step3: Now Select Memory and CPU depending upon the Usability.

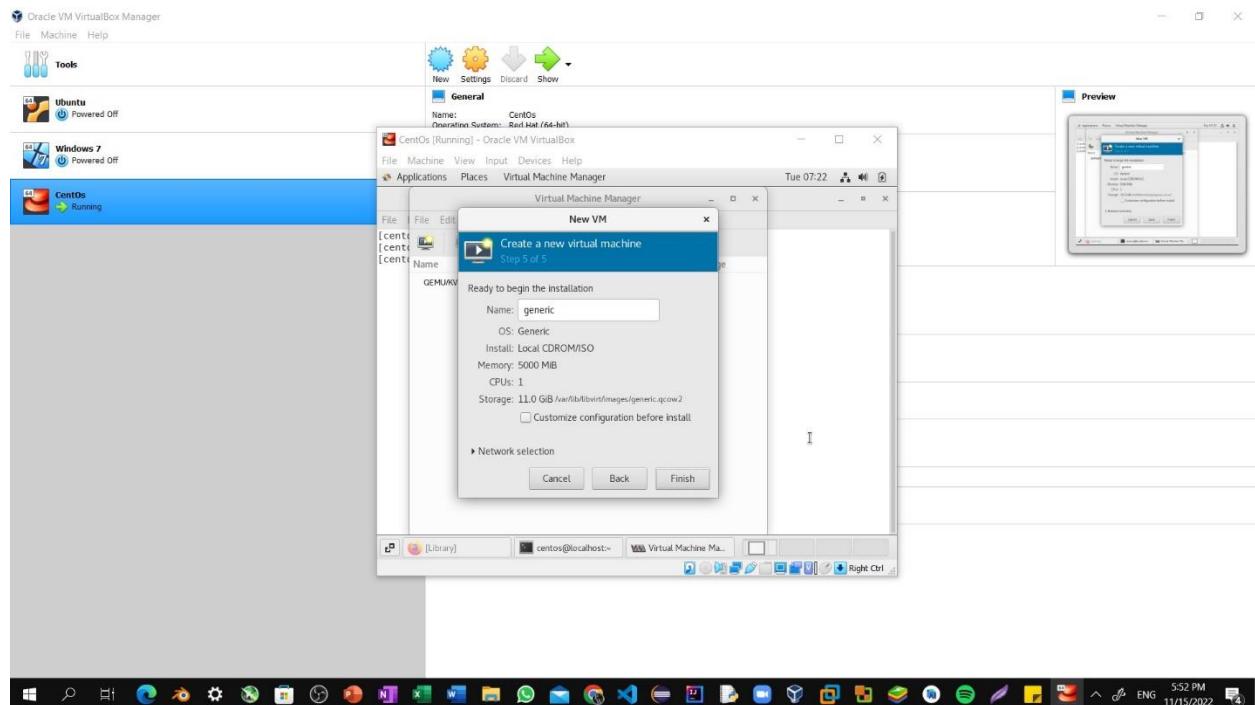


Step4: Now, Keep The default Settings as it is and then proceed further.

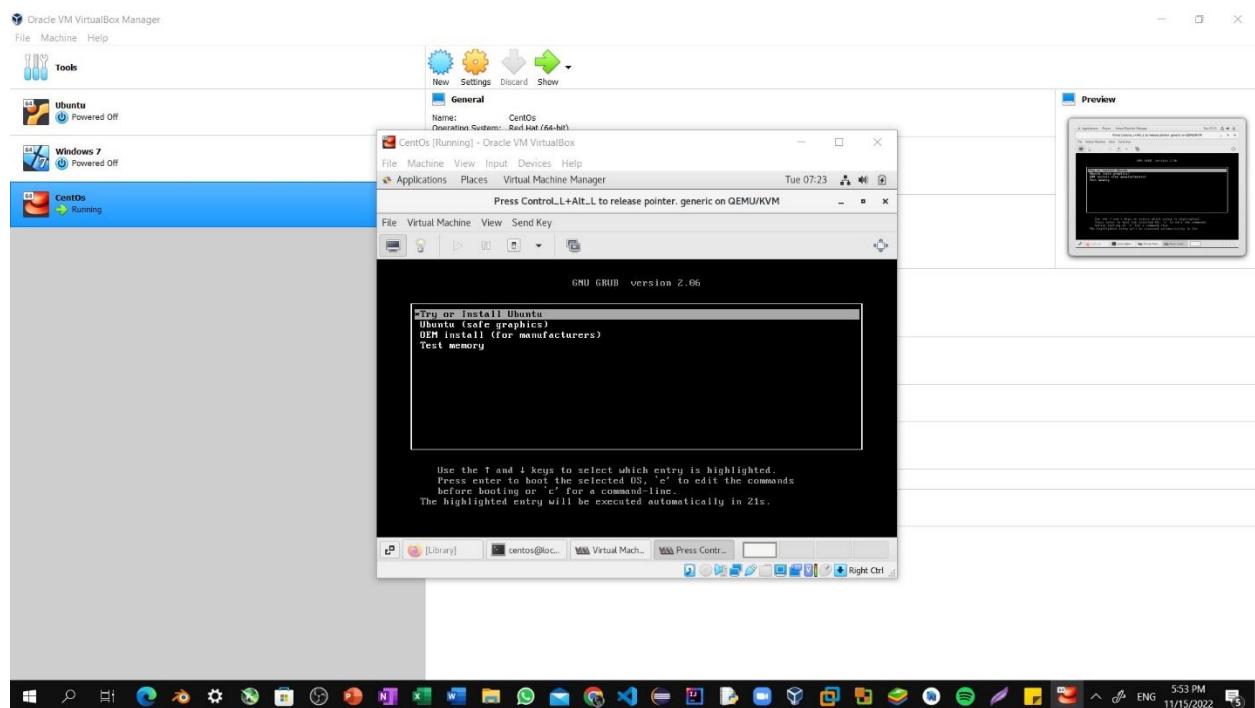


## Lab 8: Installing Ubuntu Within VM Using QEMU

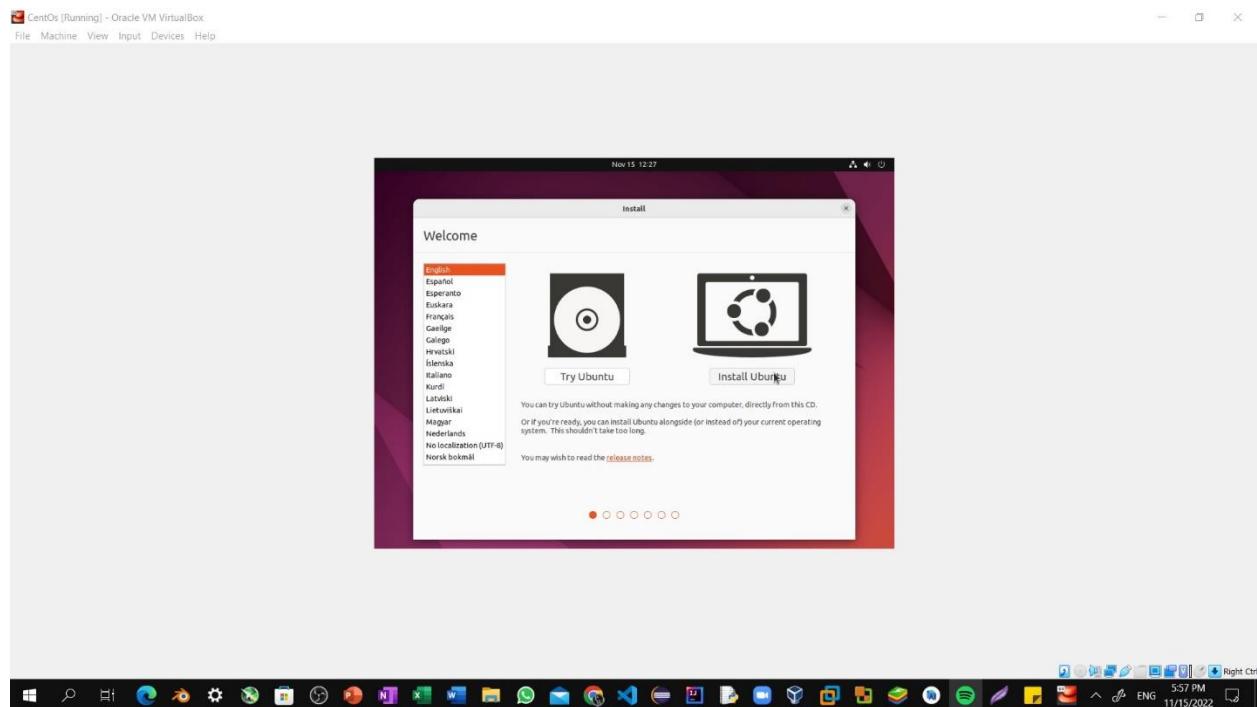
Step5: Now, Keep The default name as generic settings as it is and then Finish button.



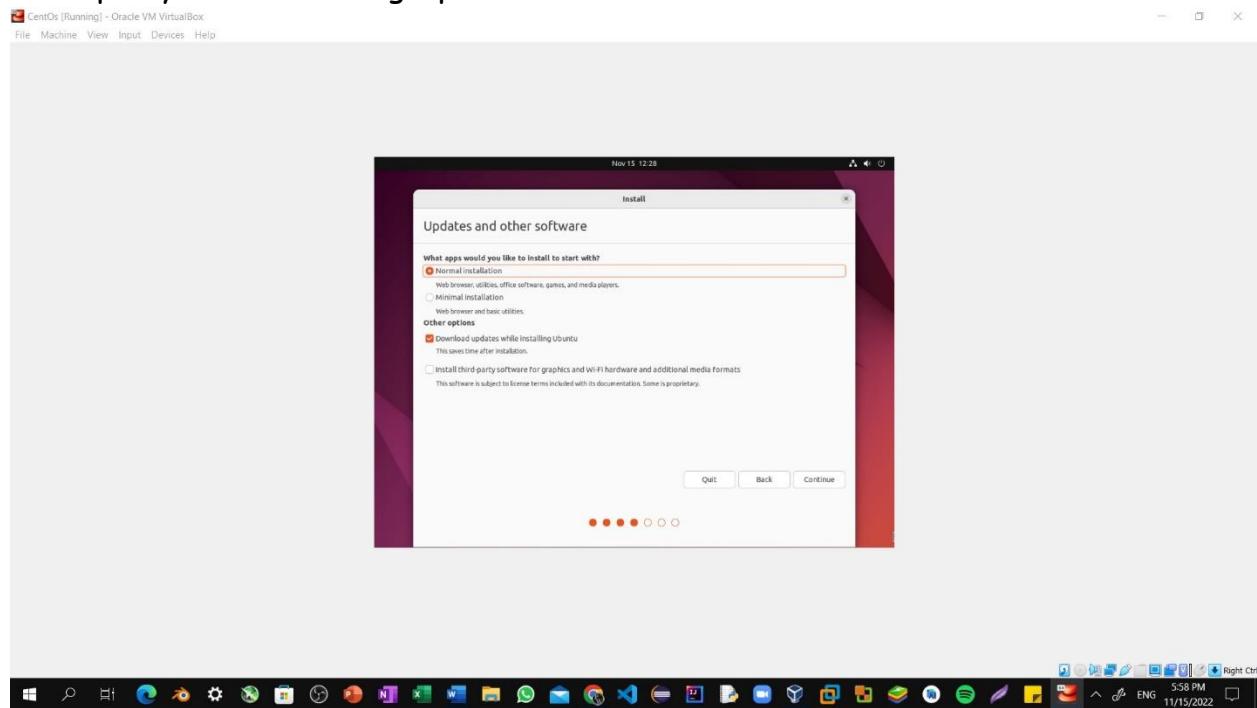
Step6: Now start the installation of virtual machine by clicking install ubuntu.



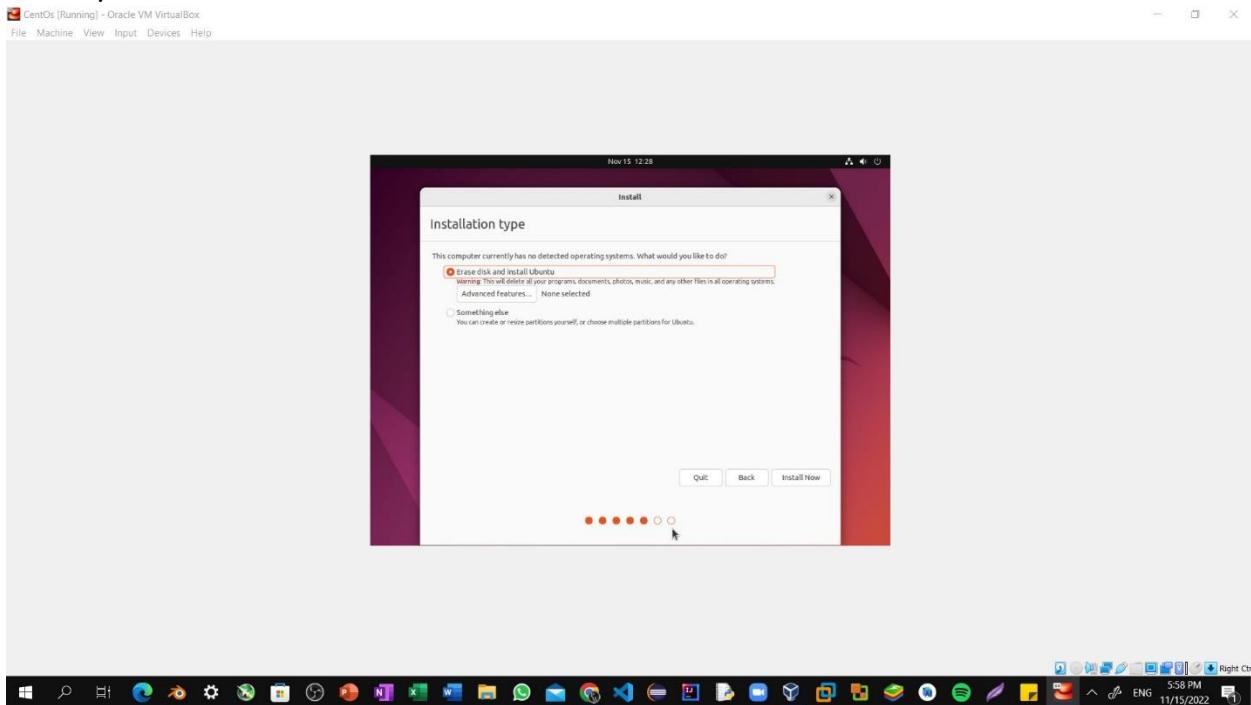
Step7: Now select English language and Click on Install Ubuntu.



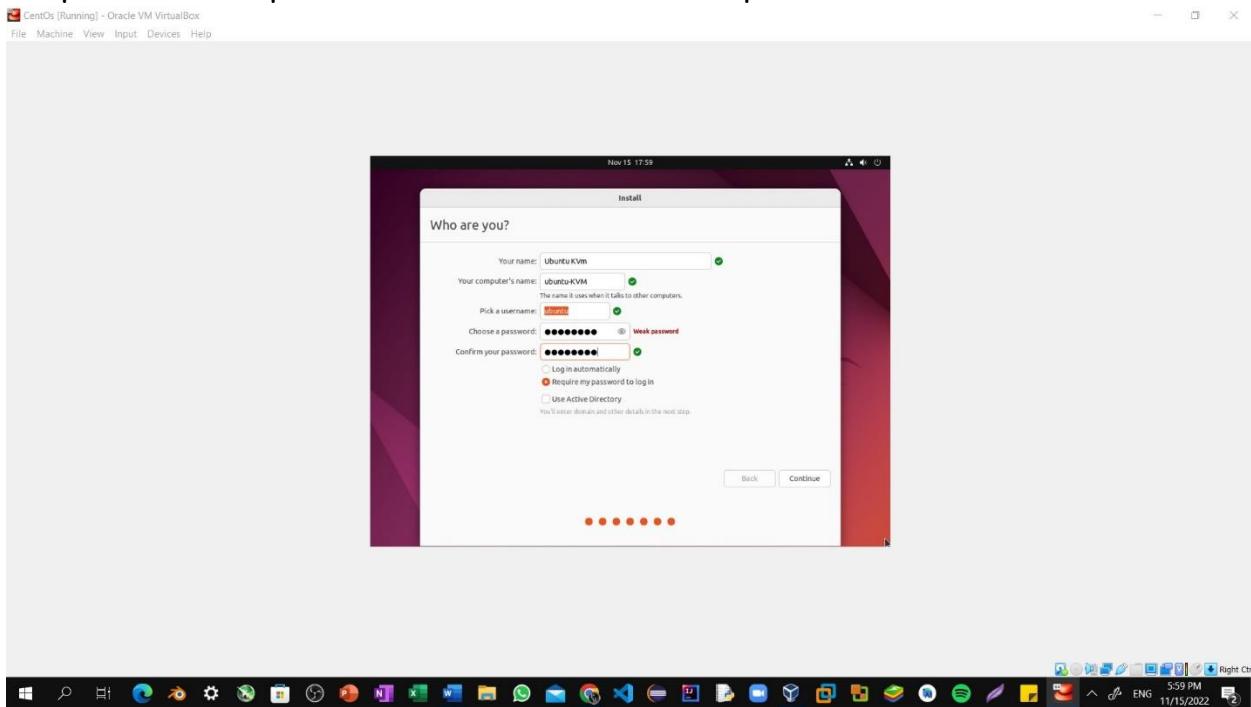
Step8: Check normal installation, download updates while installing ubuntu, install third party software for graphics and then click on next.



**Step9: Check Erase Disk and install ubuntu, this Erase Disk option doesn't affect current operating system it only make changes to Virtual Disk. Now Check Install Now option.**

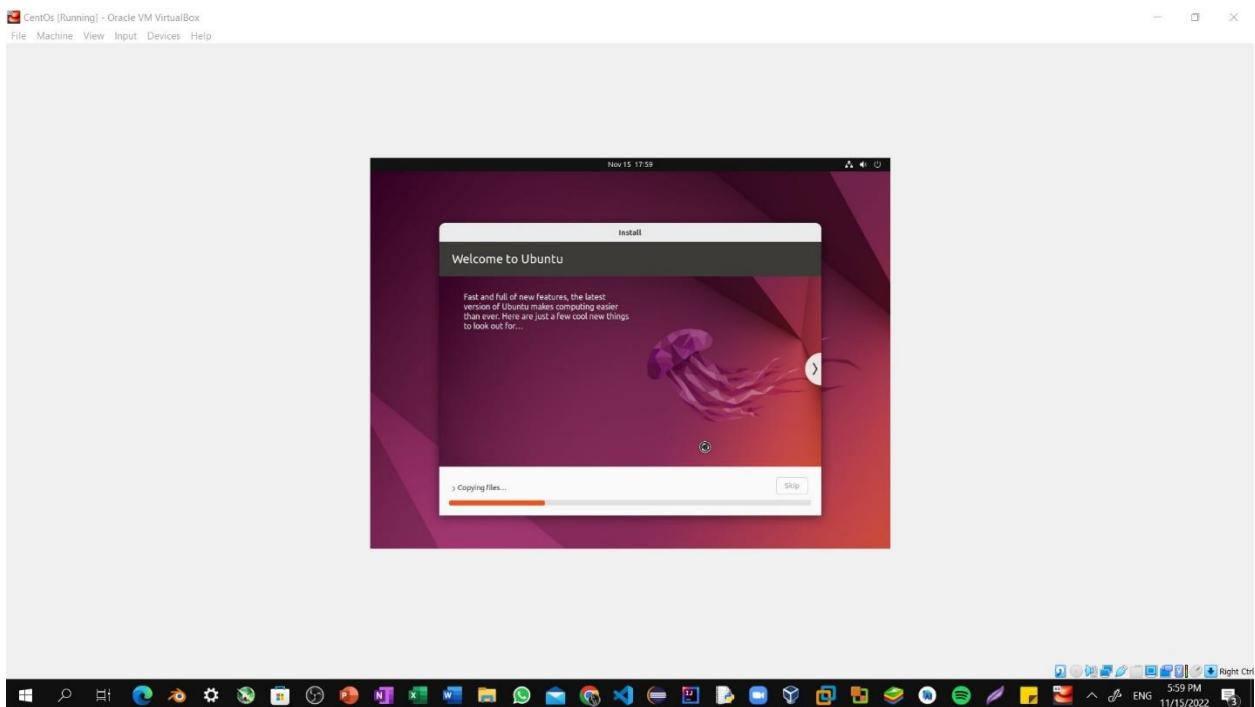


**Step10: Now setup virtual machine username and password.**

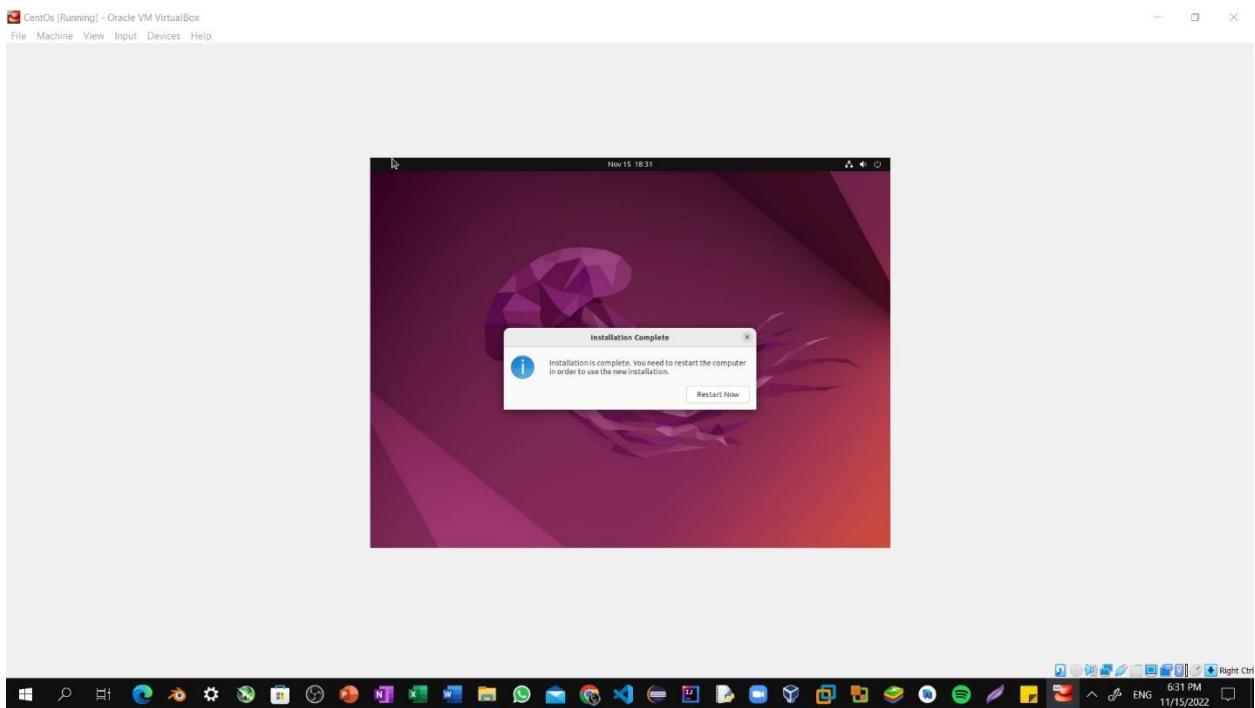


## Lab 8: Installing Ubuntu Within VM Using QEMU

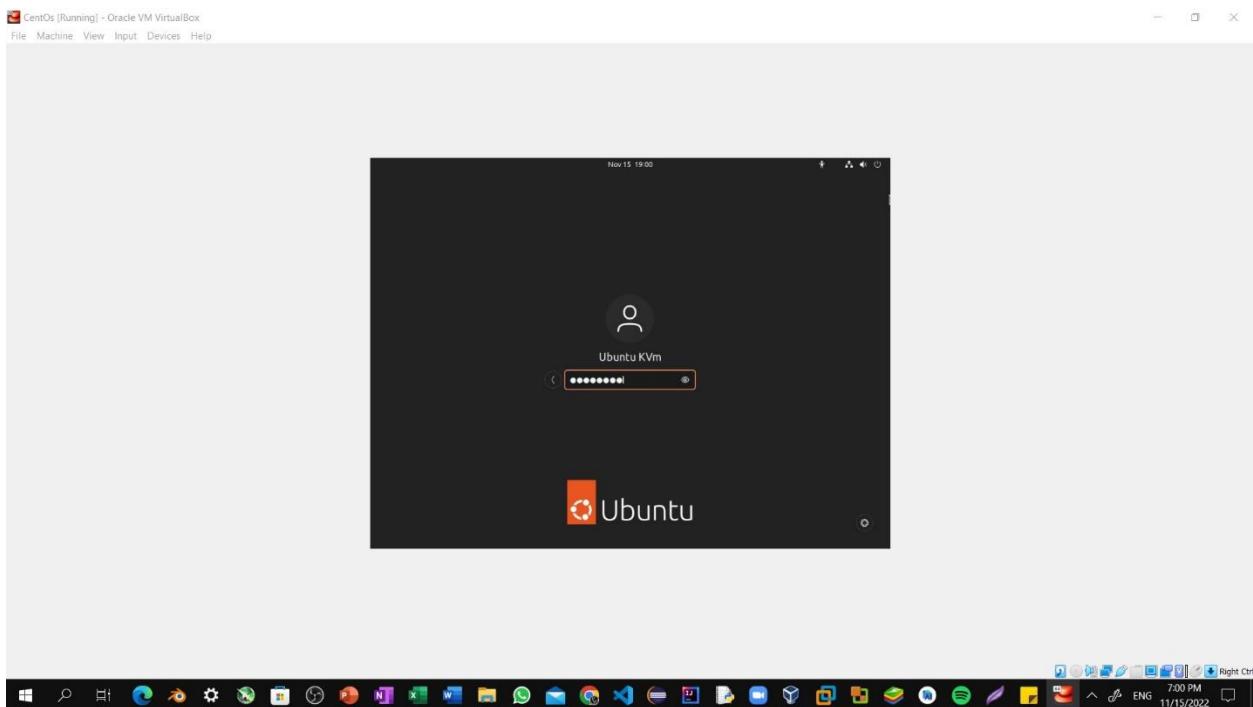
Step11: Now wait for few minutes until installation get completed.



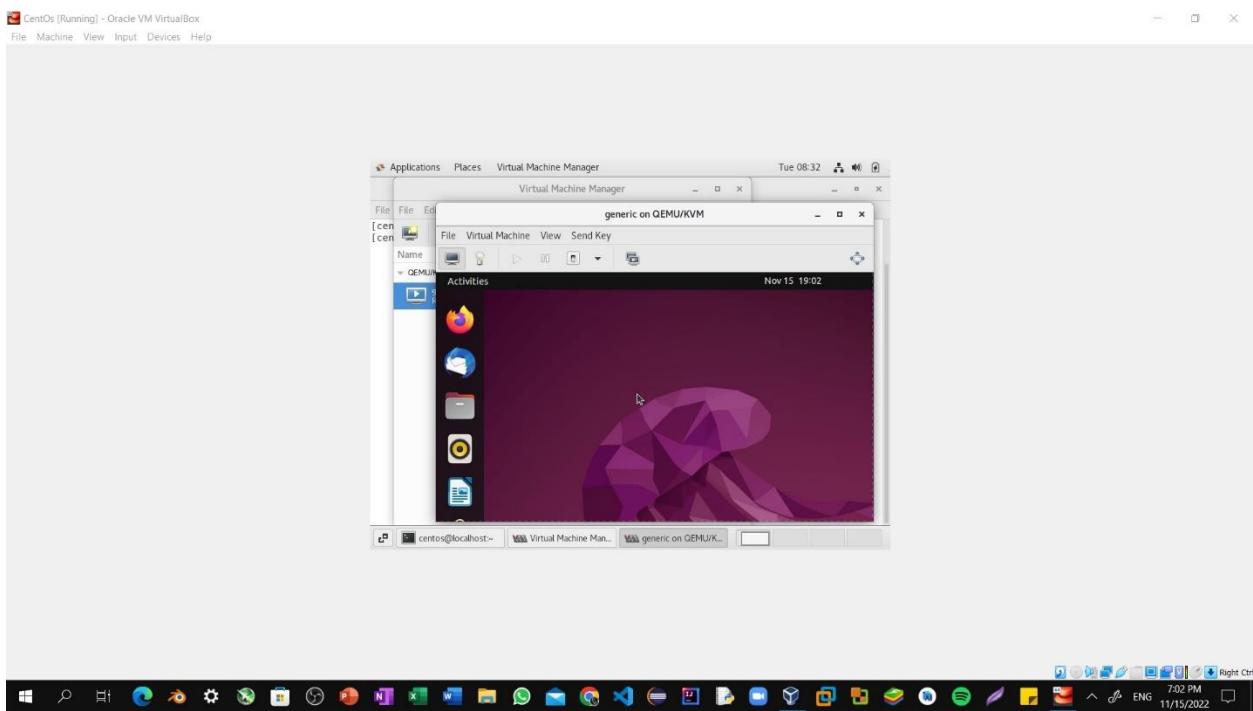
Step12: Once the installation is completed. We need to restart Virtual machine in order to use.



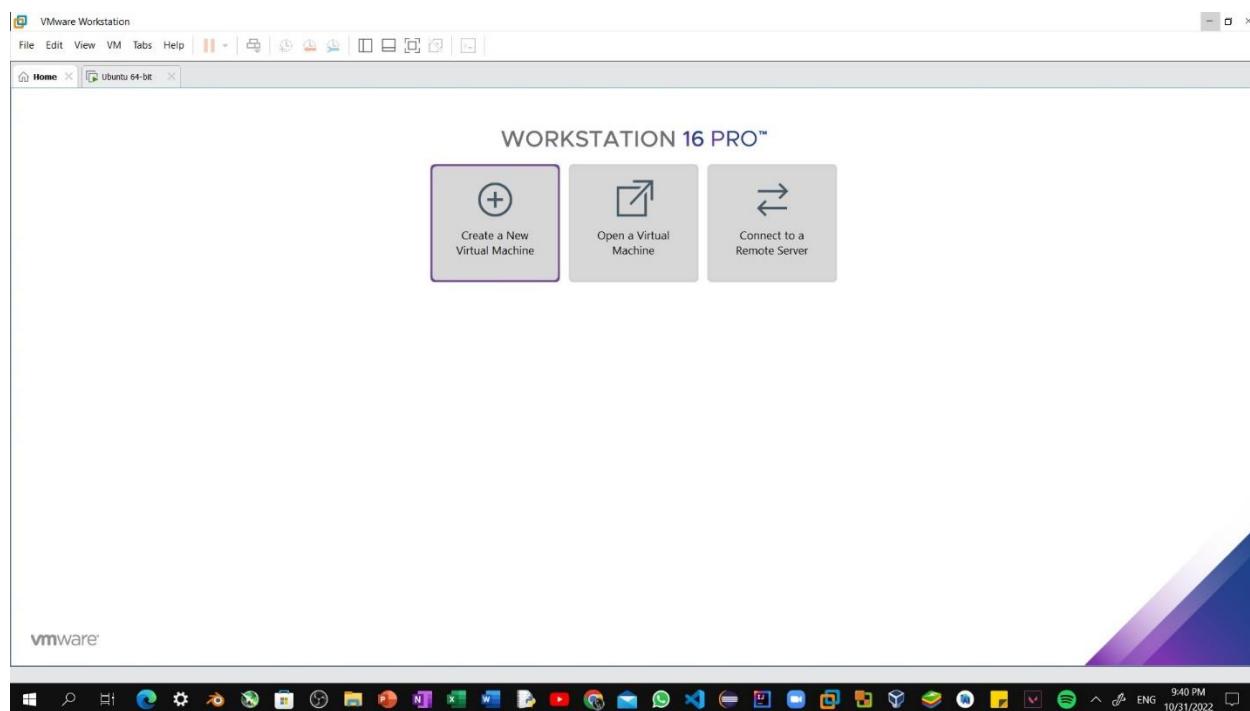
Step13: Now, Enter your password and login to your workspace.



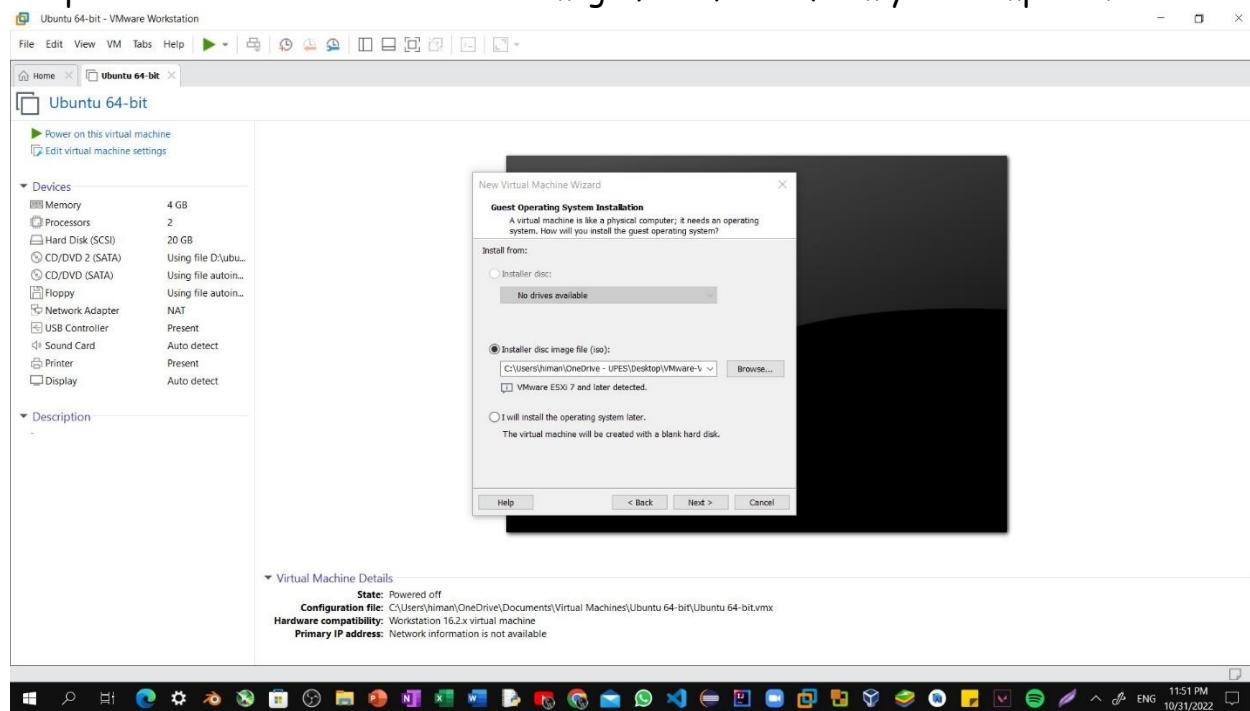
Step14: Ubuntu Workspace.



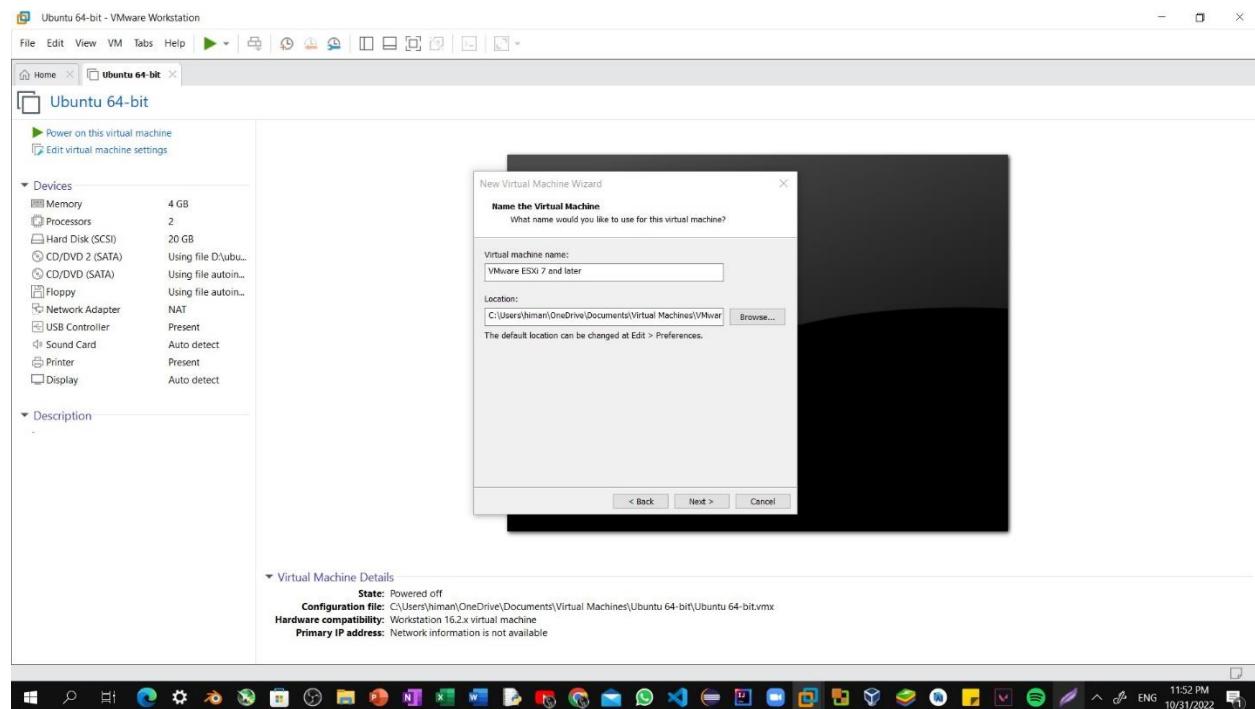
Step1: Open Workstation pro click on Create a new Virtual machine.



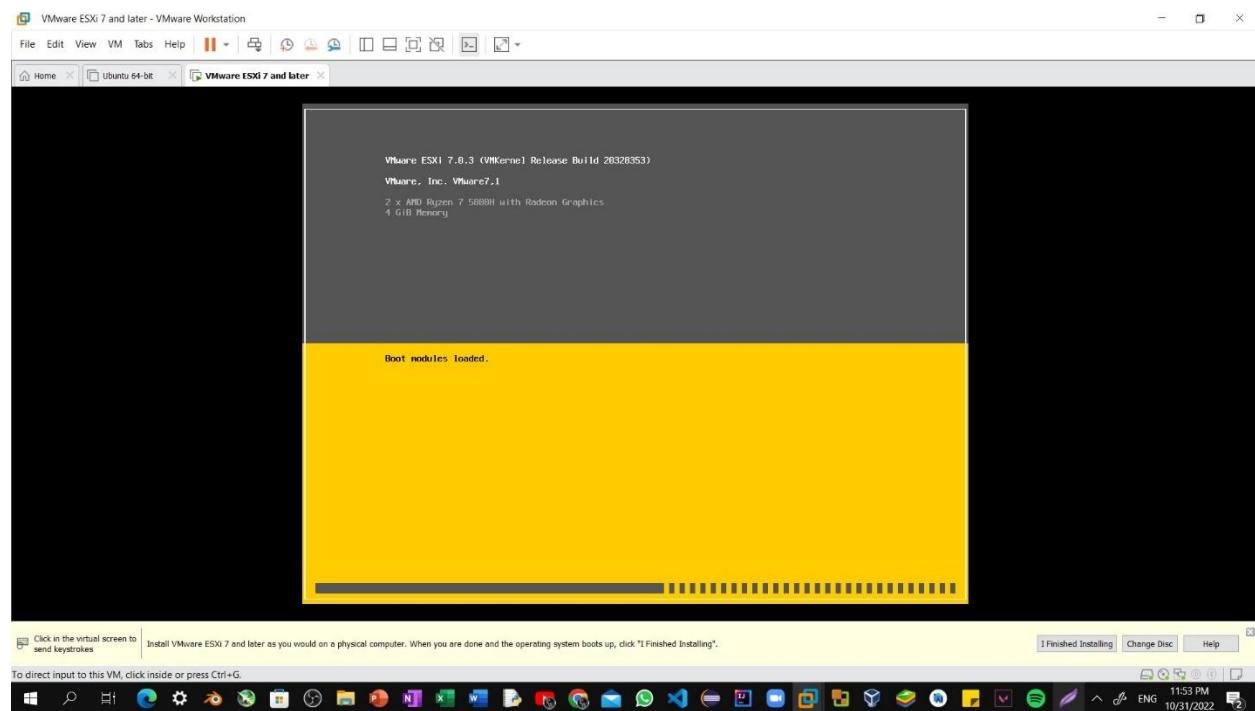
Step2: Select the downloaded disc image file of esxi from your computer.



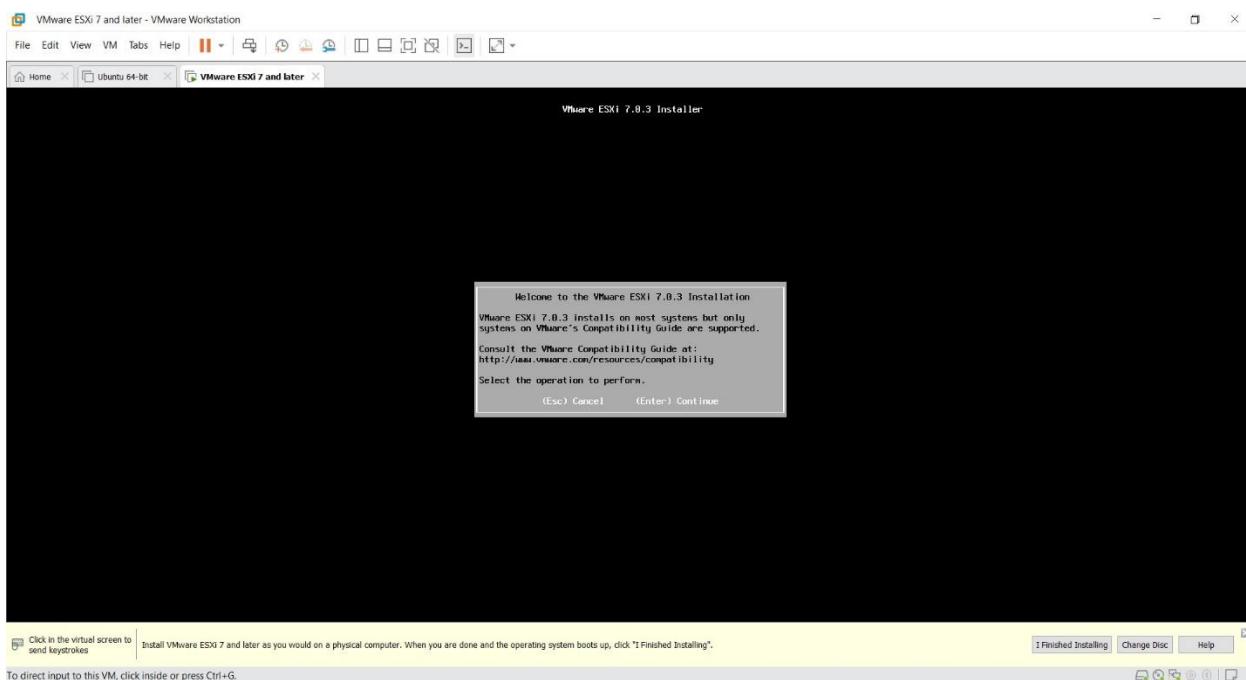
## Step3: Selecting iso file of ESxi.



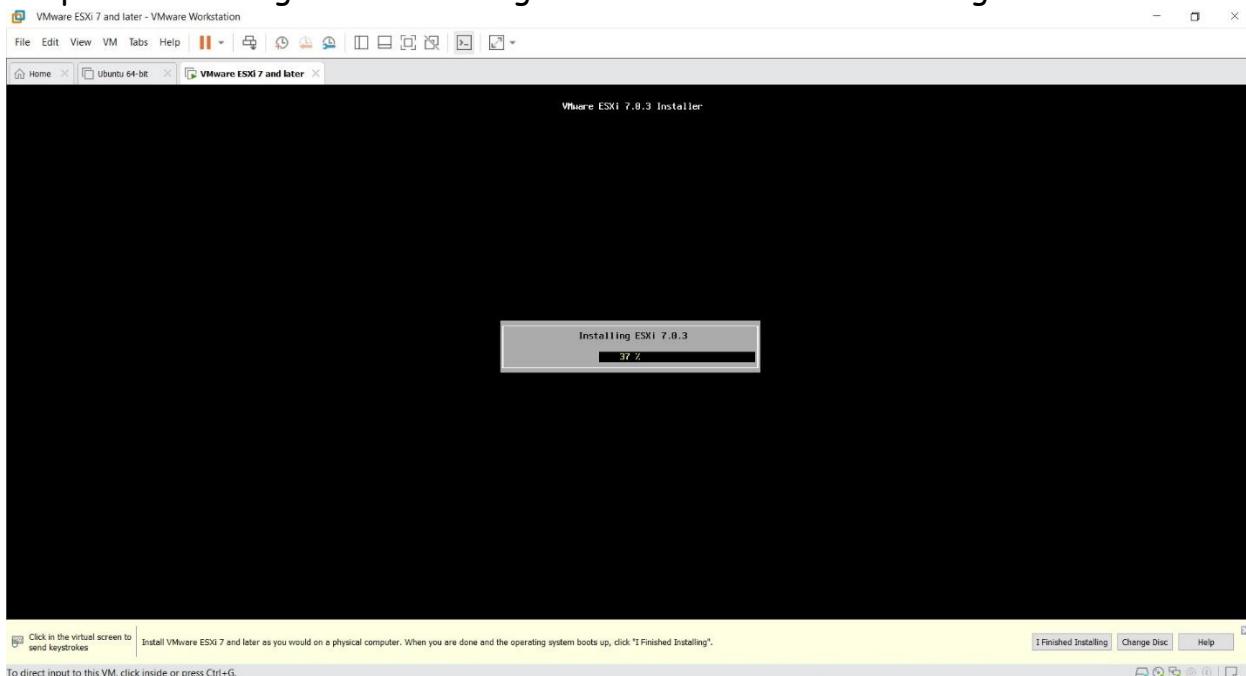
## Step4: The installation has been started.



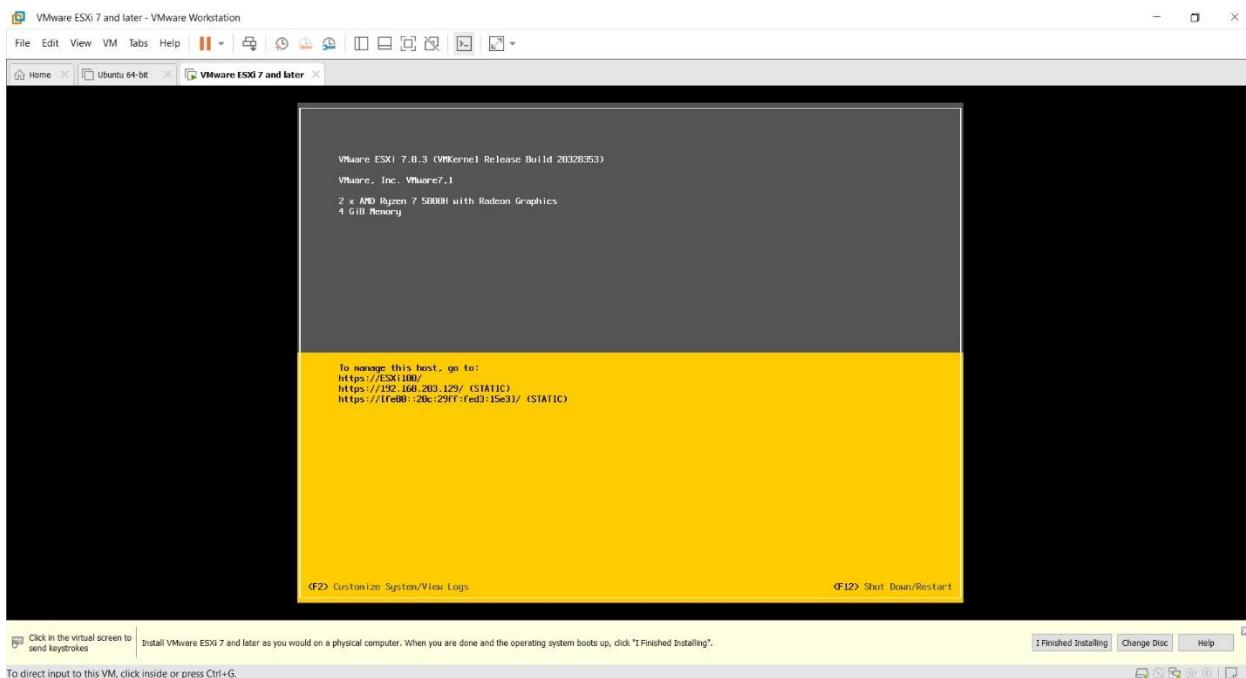
Step5: Click on continue option.



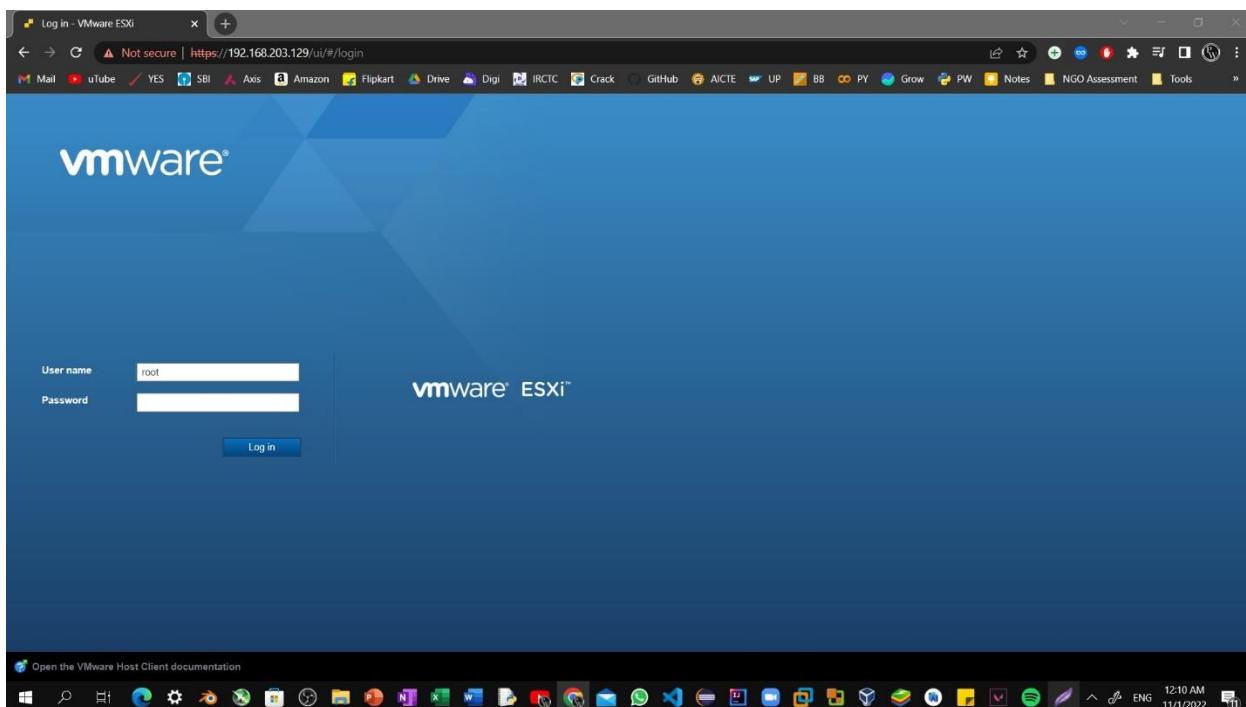
Step6: After doing further settings the installation will start begin.



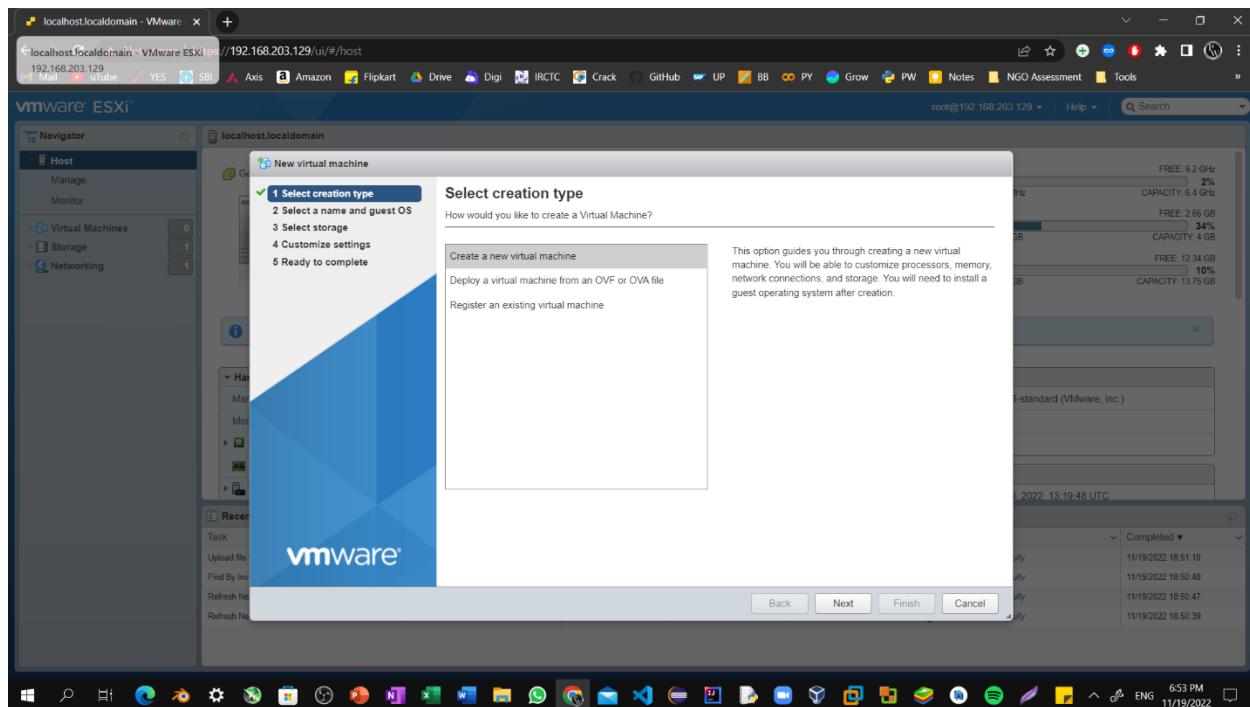
Step7: After installing esxi on workstation pro you will find your own site which you have type on google.



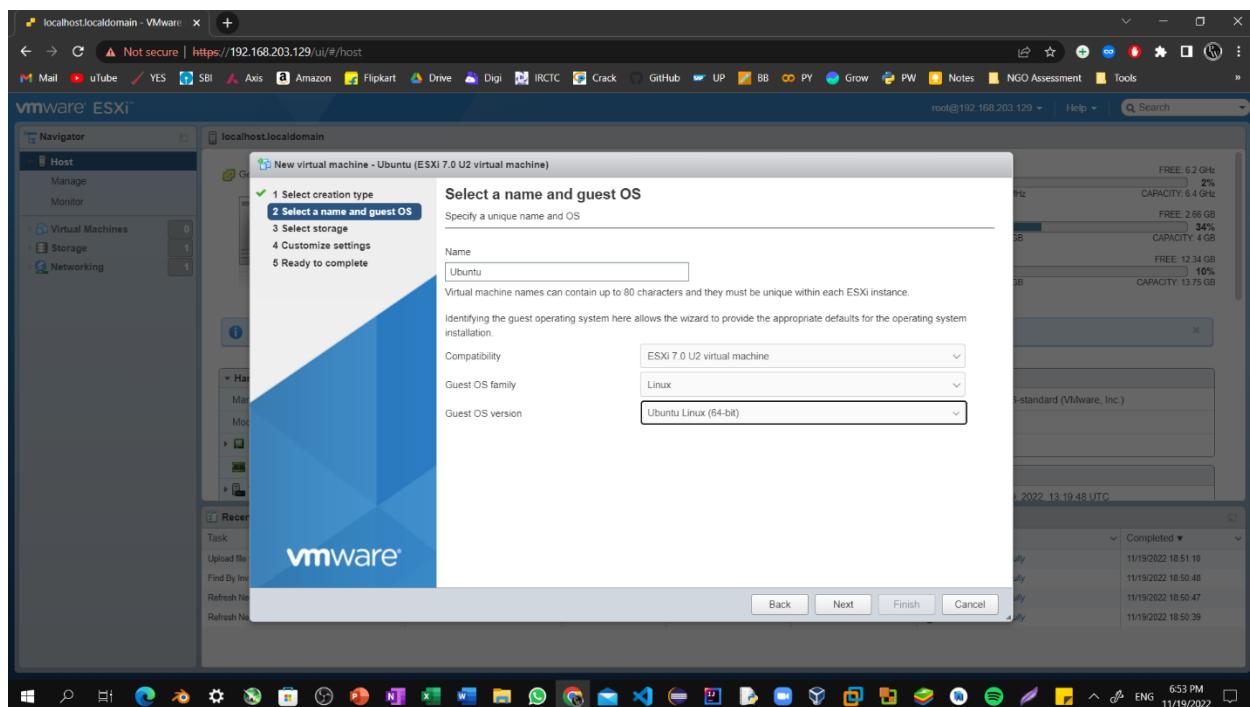
Step8: Open ip address on any web browser.



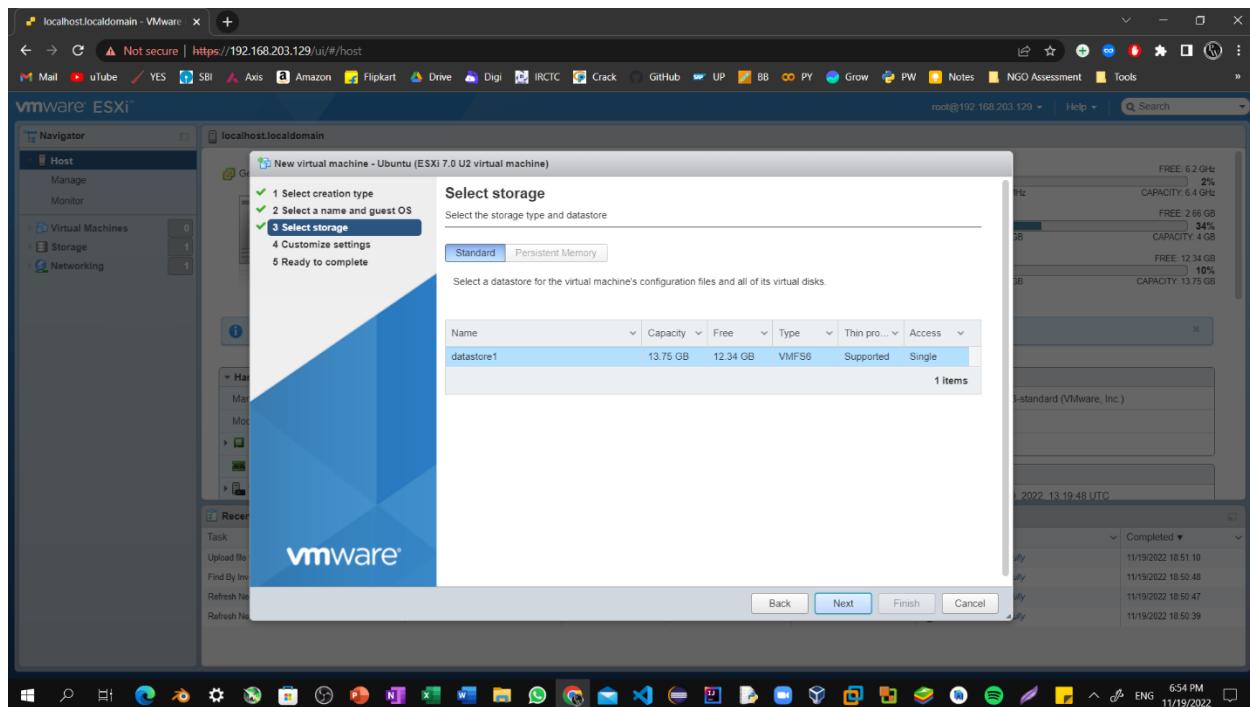
Step9: Right click on host click on to create new virtual machine.



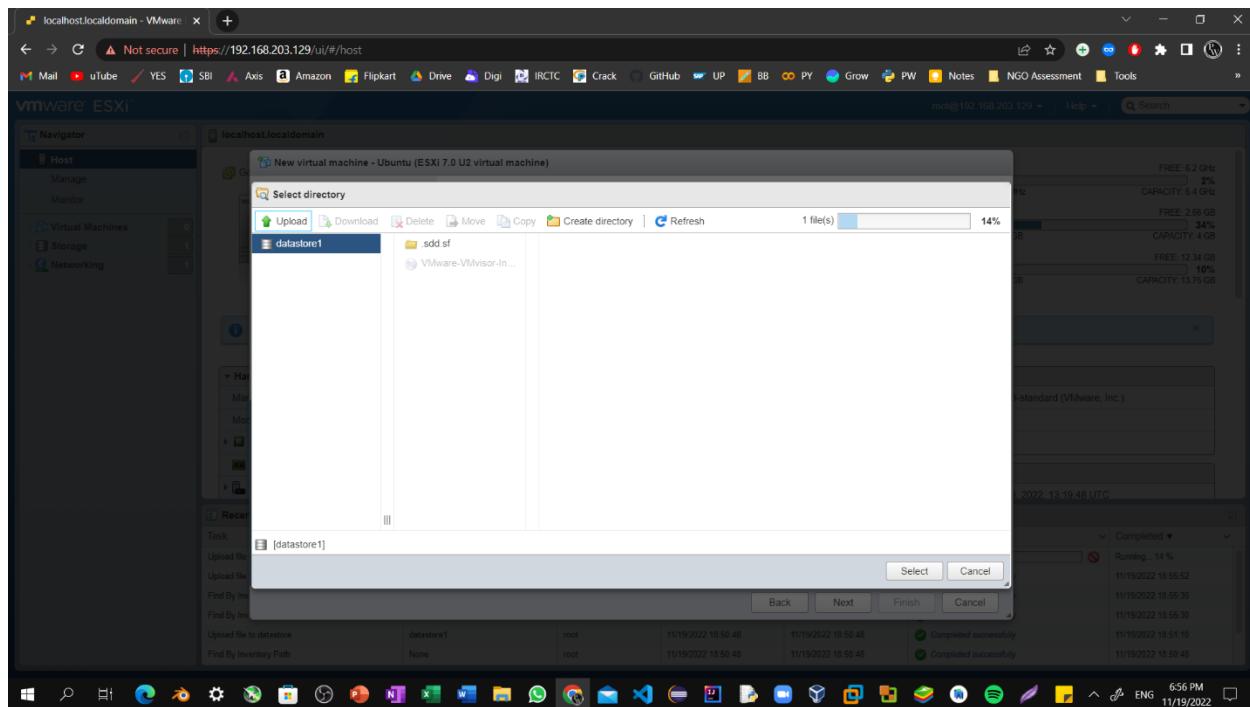
Step10: Choose the virtual machine name, its guest os and guest os version.



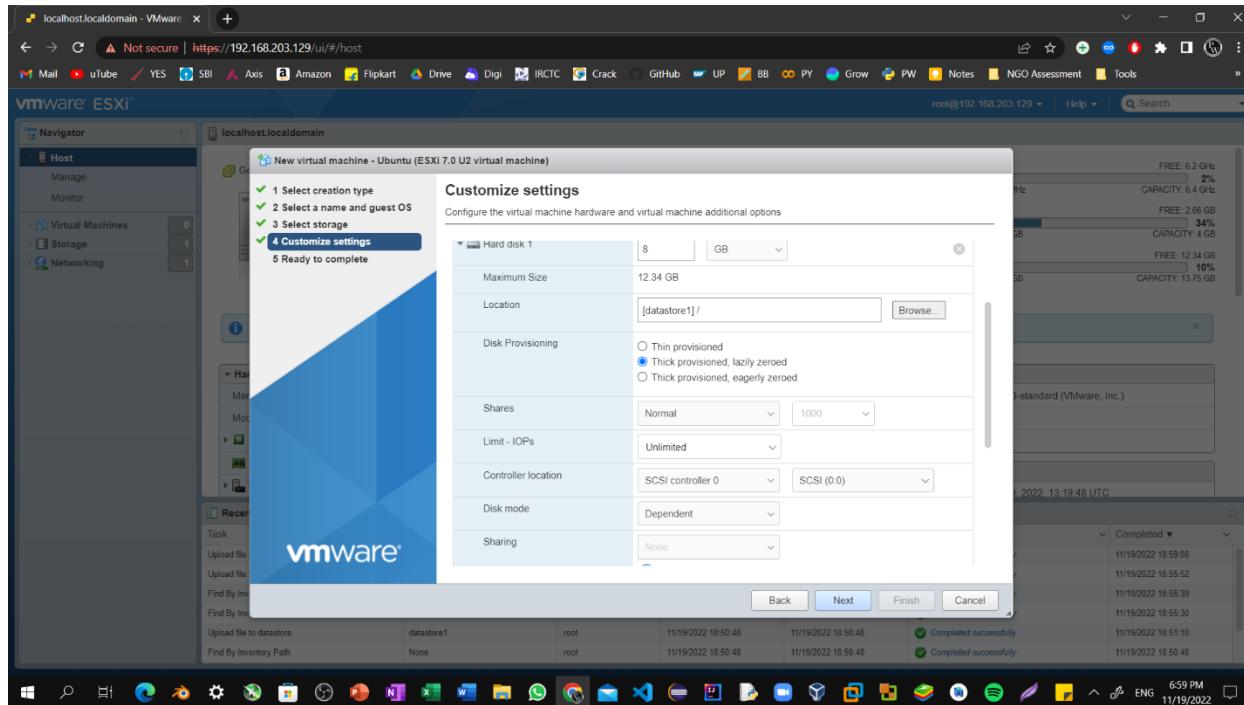
Step11: Proceed Further by clicking on next.



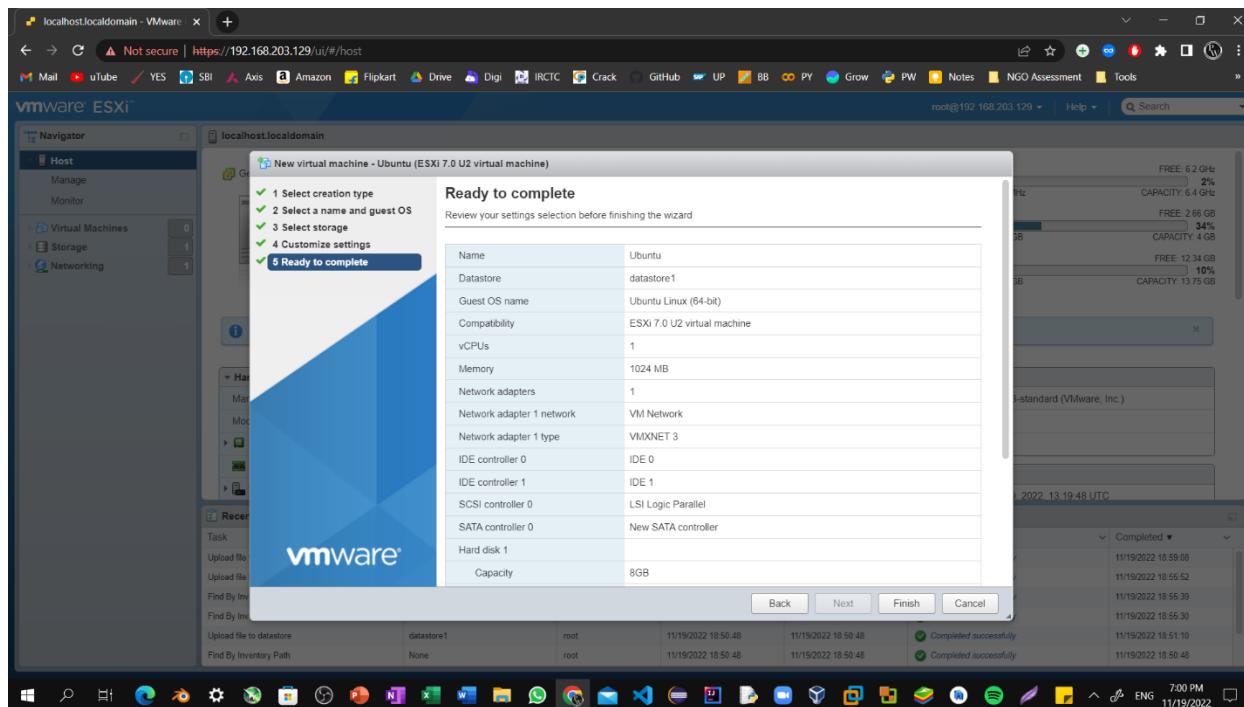
Step12: Upload VM file of Ubuntu by clicking over upload button.



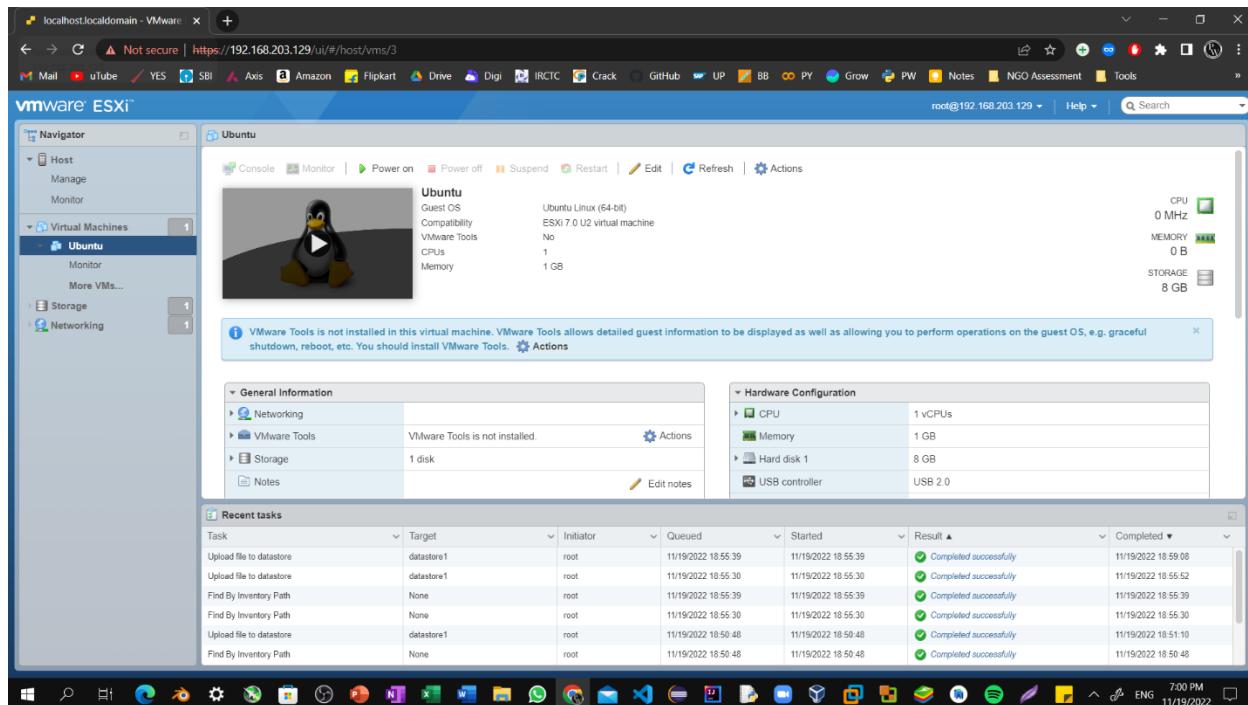
Step12: Customize the required cpu, memory and select the iso file of your virtual machine.



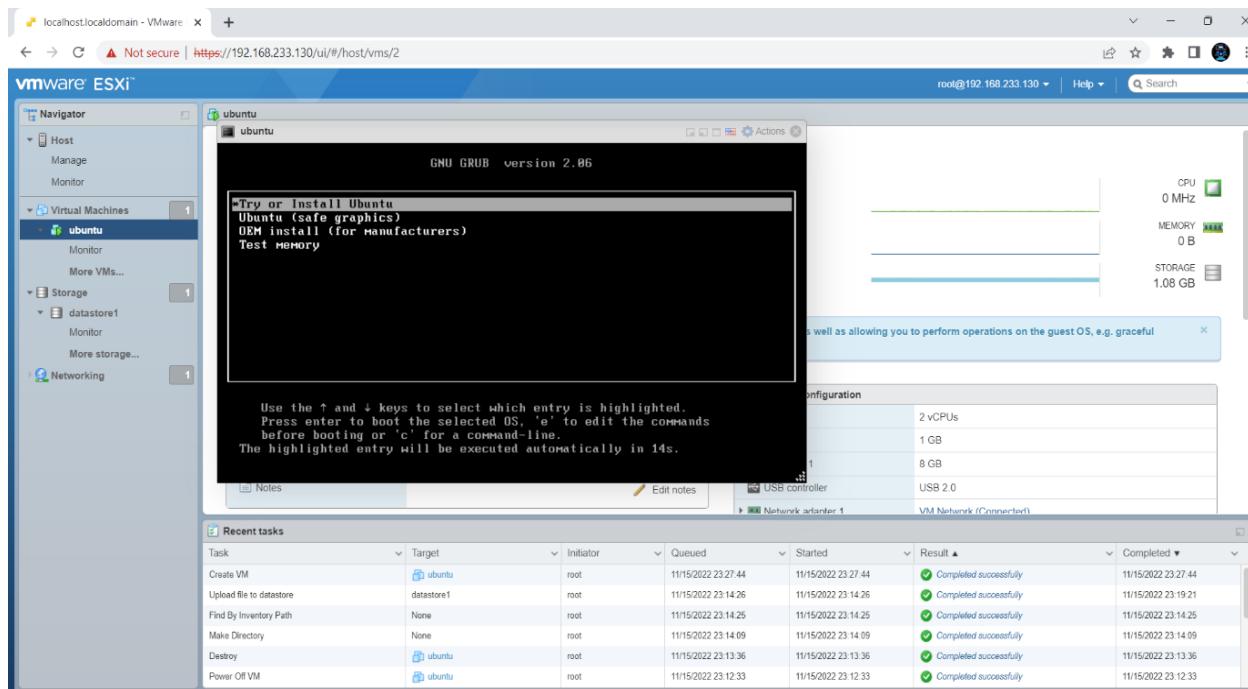
Step13: Click on Finish and to proceed further.



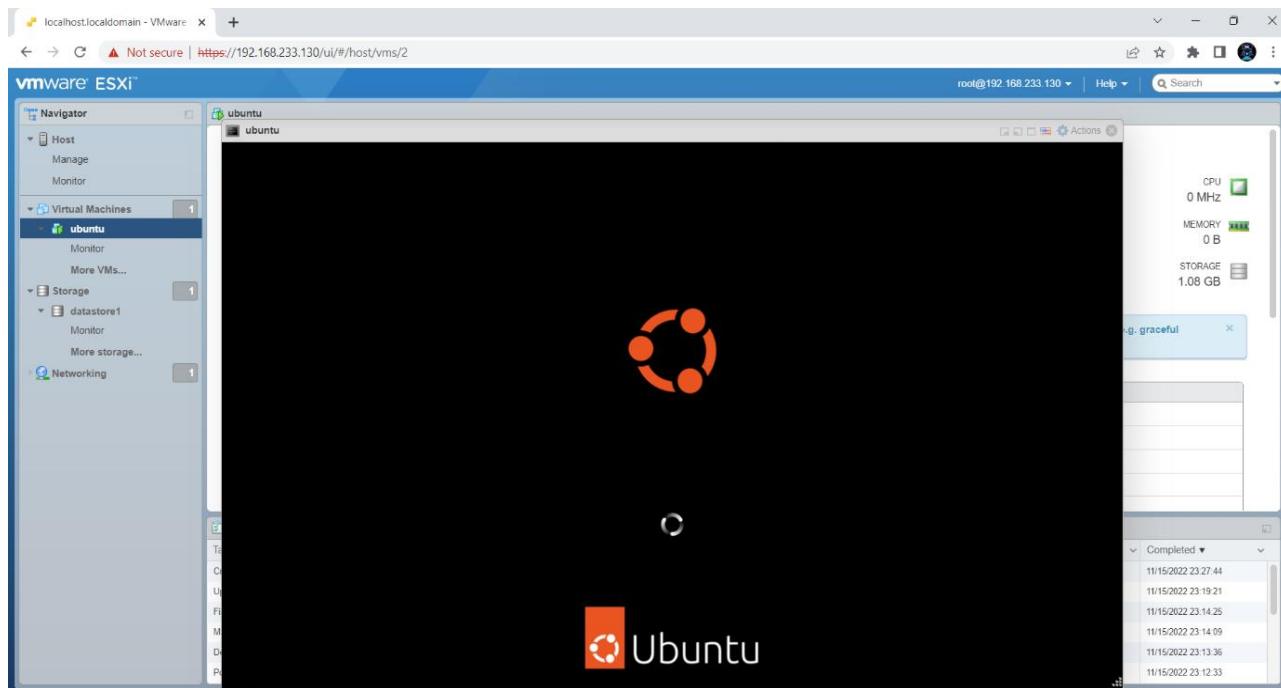
Step14: Now go to virtual machine tab where you find the virtual machine which is created by you.



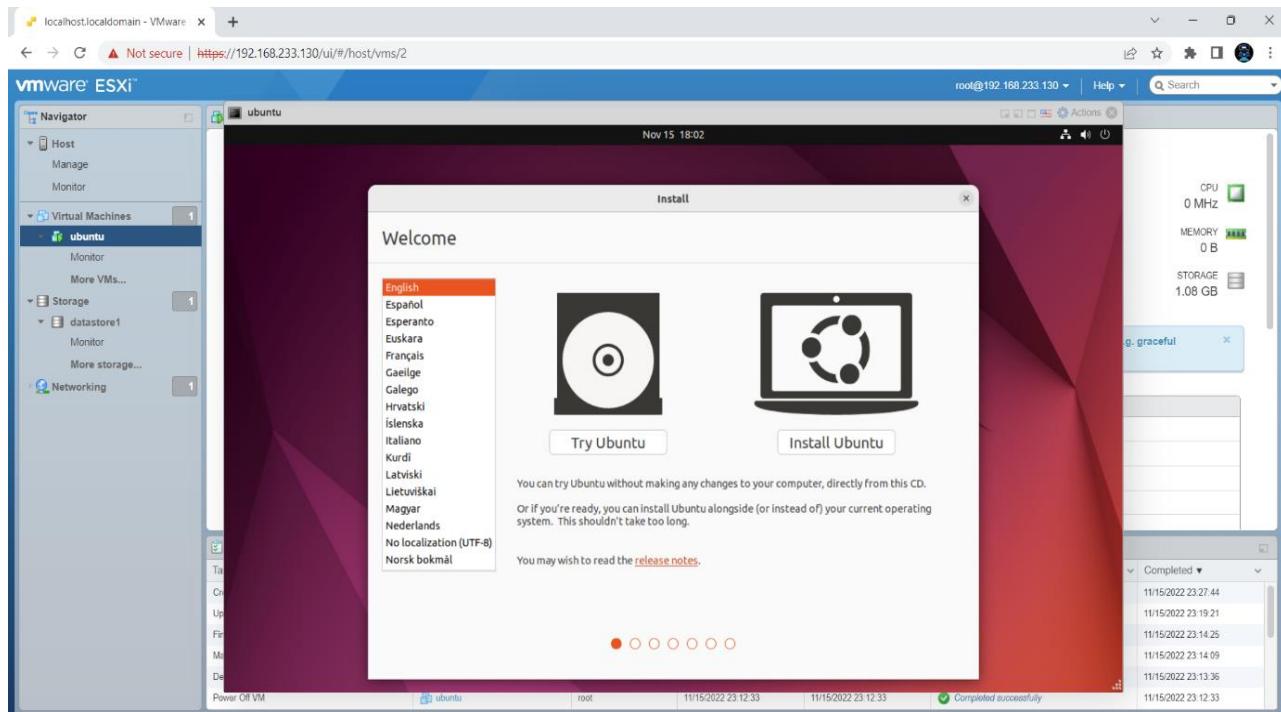
Step15: Click on virtual machine's image and it will start installing.



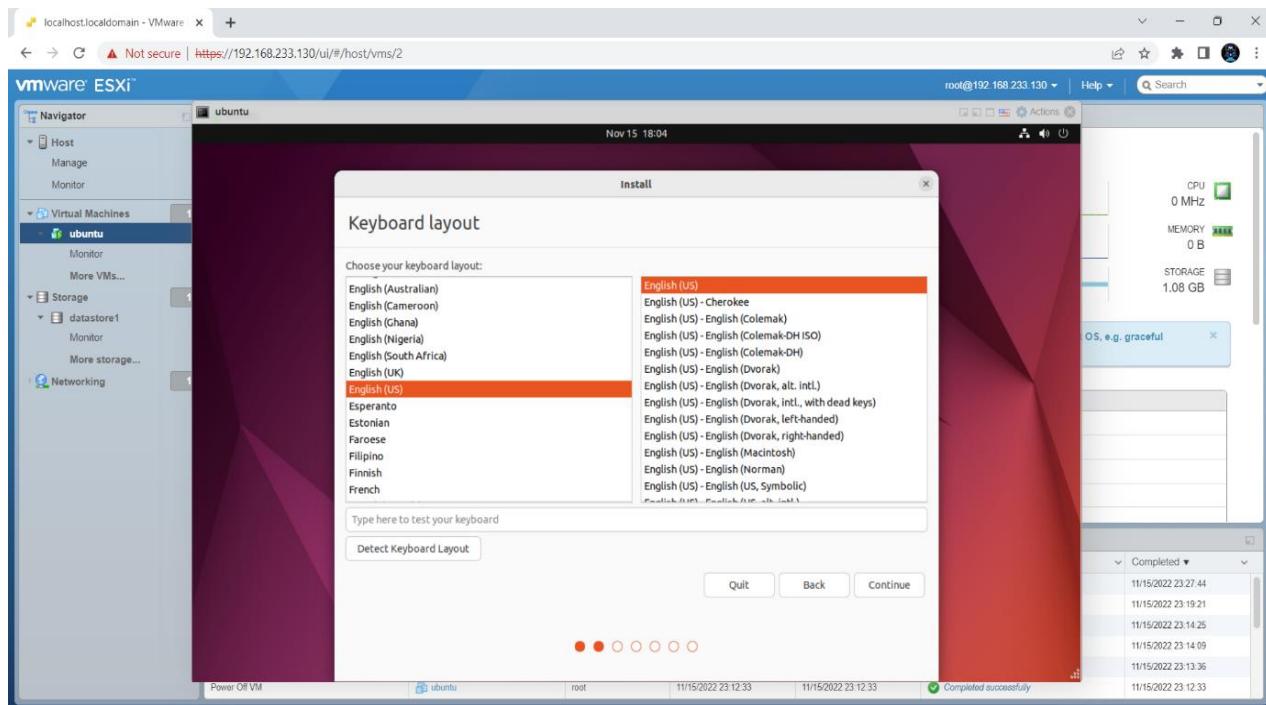
Step16: Now your virtual machine is installing on esxi.



Step17: Now the virtual machine had been successfully installed on esxi.

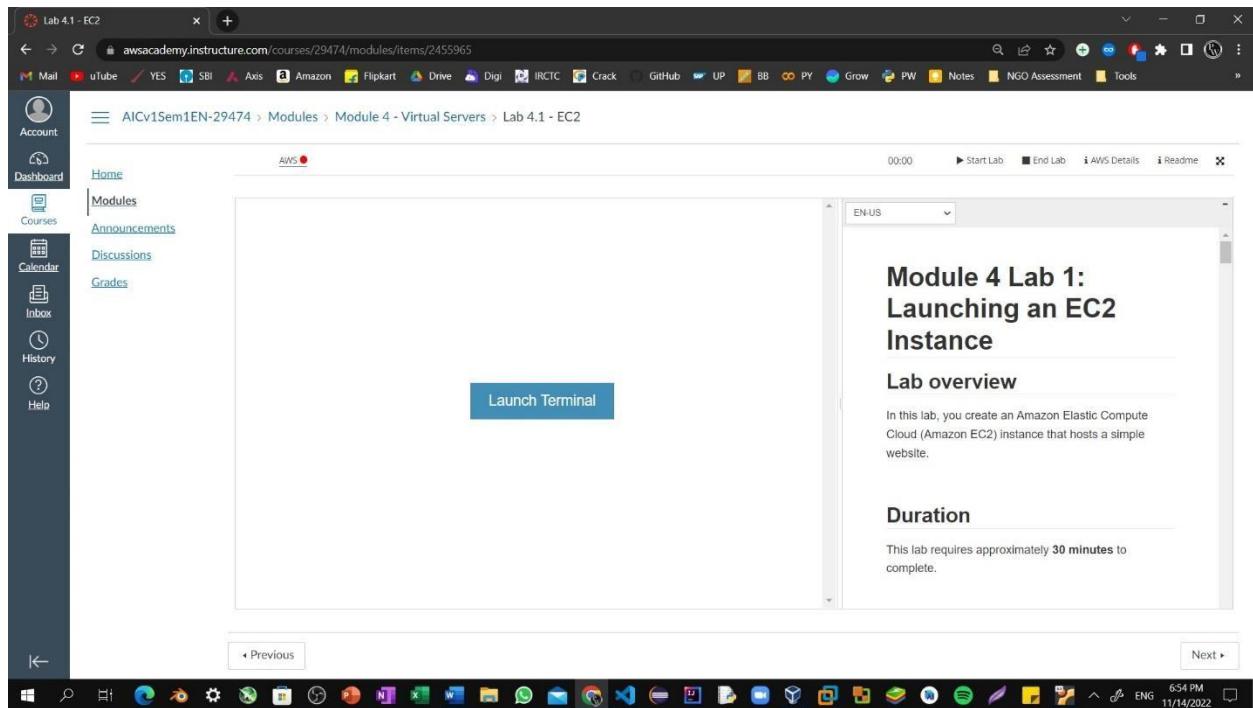


Step18: You can select language to stat further your virtual machine.

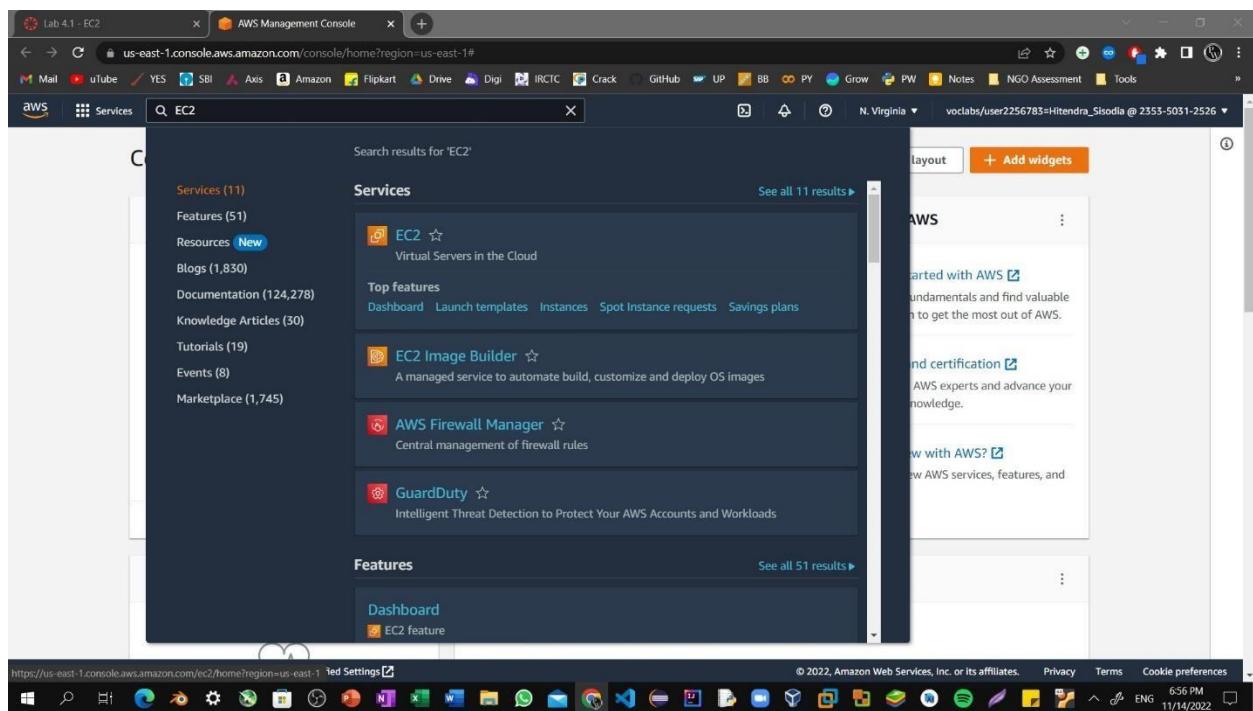


## Lab 10.1: Launching an EC2

Step1: To start the lab session, choose **Start Lab** in the upper-right corner of the page.



Step2: Choose the **Services** menu, locate the **Compute** services, and select **EC2**.



## Lab 10.1: Launching an EC2

Step3: Choose the **Launch instance** button in the middle of the page, and then select **Launch instance** from the dropdown menu.

The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with 'EC2 Dashboard', 'Instances' (selected), 'Images', and other services like 'Amazon CloudWatch Metrics'. The main area has a 'Launch instance' button highlighted in orange. To its right is a 'Service health' section showing 'US East (N. Virginia)' is operating normally. Below that is a 'Zones' table with four rows: us-east-1a, us-east-1b, us-east-1c, and us-east-1d, each associated with zone ID use1-az1, use1-az2, use1-az4, and use1-az6 respectively. On the far right, there's an 'Explore AWS' sidebar with links to cost reduction, GuardDuty, Graviton2, and additional information.

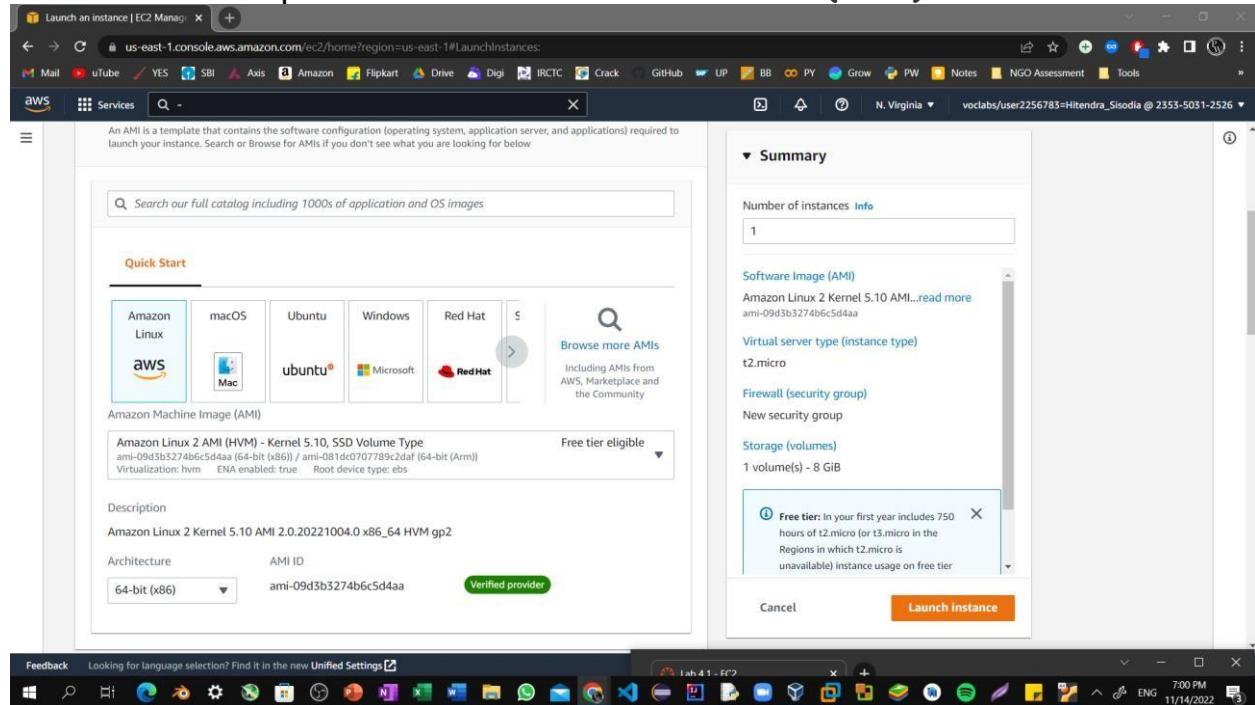
Step4: Name the instance i.e, Hitendra Sisodia.

The screenshot shows the 'Launch an instance' wizard. In the 'Name and tags' step, the name 'HitendraSisodia' is entered in the 'Name' field. The 'Summary' panel on the right shows 'Number of instances' set to 1. It also lists the 'Software Image (AMI)', 'Virtual server type (instance type)', 'Firewall (security group)', 'Storage (volumes)', and a note about the 'Free tier'. At the bottom right is a large orange 'Launch instance' button.

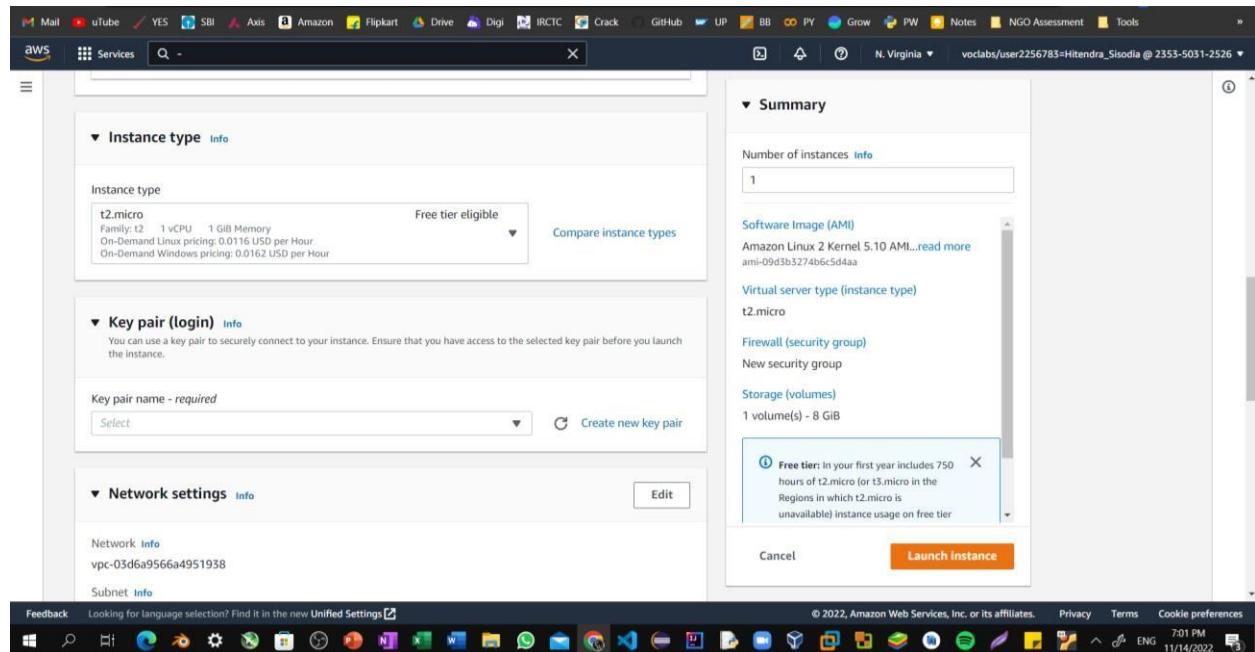
## Lab 10.1: Launching an EC2

**Step5: Choose an AMI from which to create the instance:**

In the list of available Quick Start AMIs, keep the default Amazon Linux AMI selected. Also keep the default Amazon Linux 2 AMI (HVM) selected.

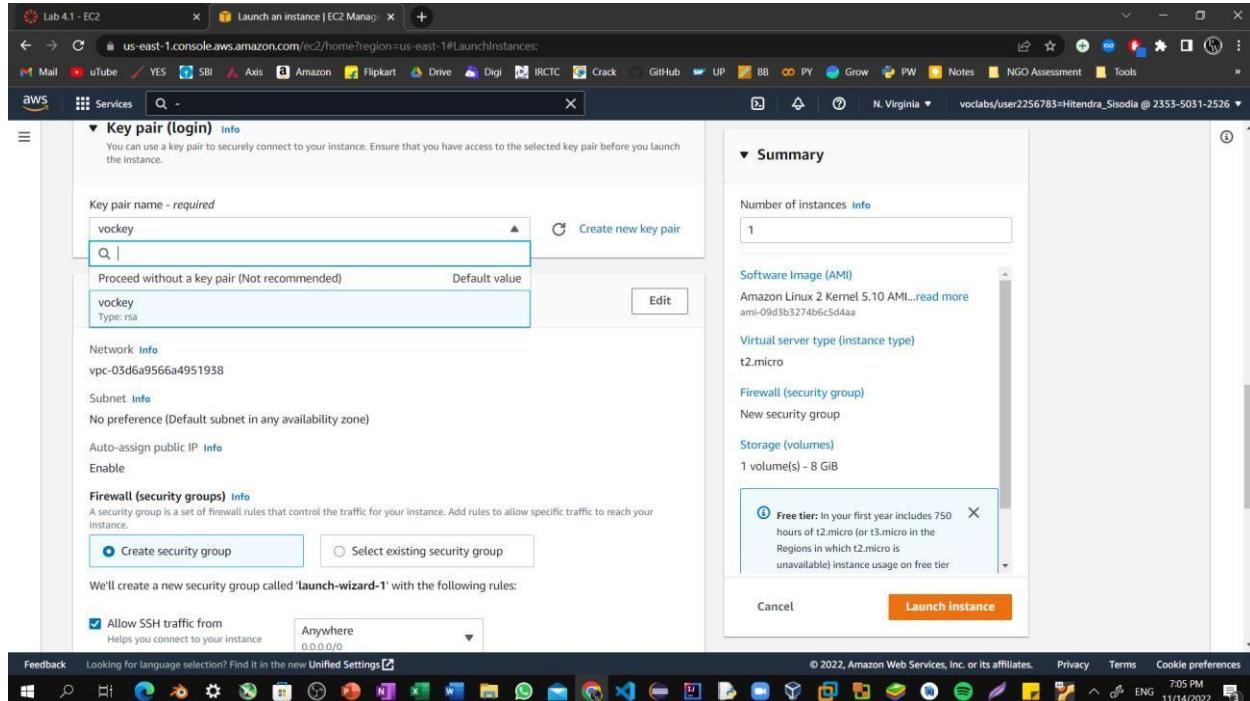


**Step6: Specify an Instance type: In the Instance type panel, keep the default t2.micro selected.**

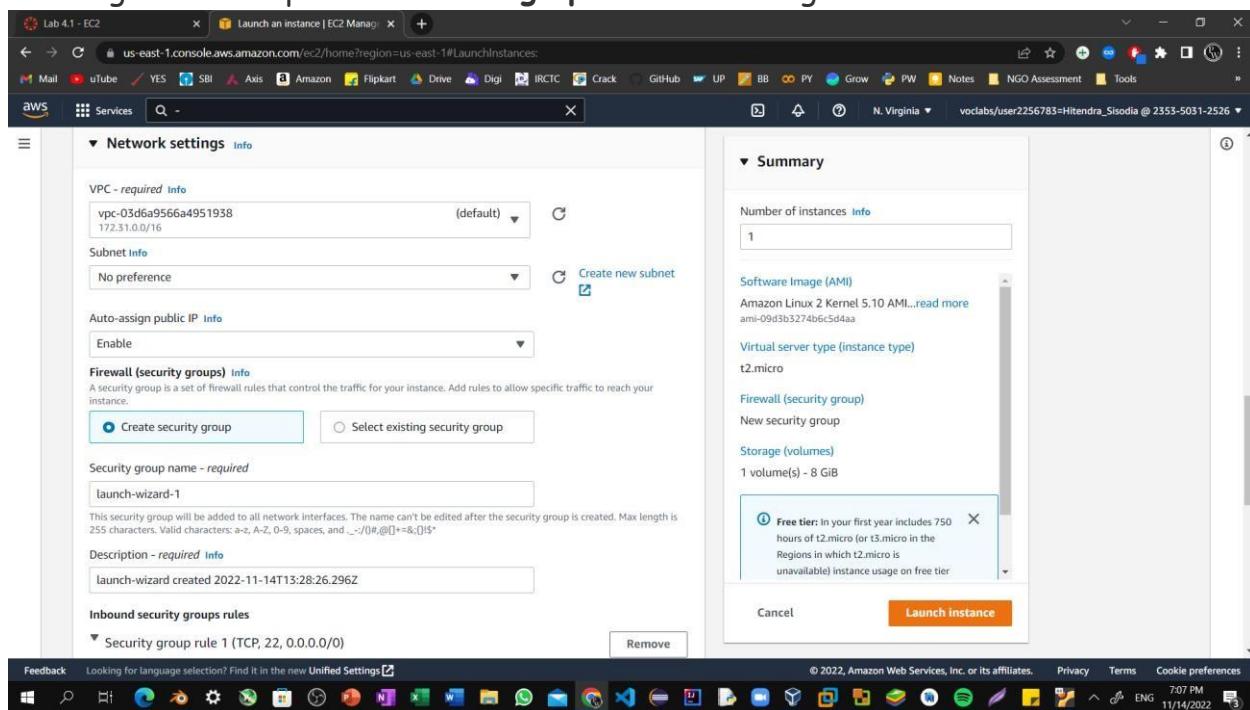


## Lab 10.1: Launching an EC2

**Step7:** Select the key pair to associate with the instance. From the Key pair name menu, select **vockey**.

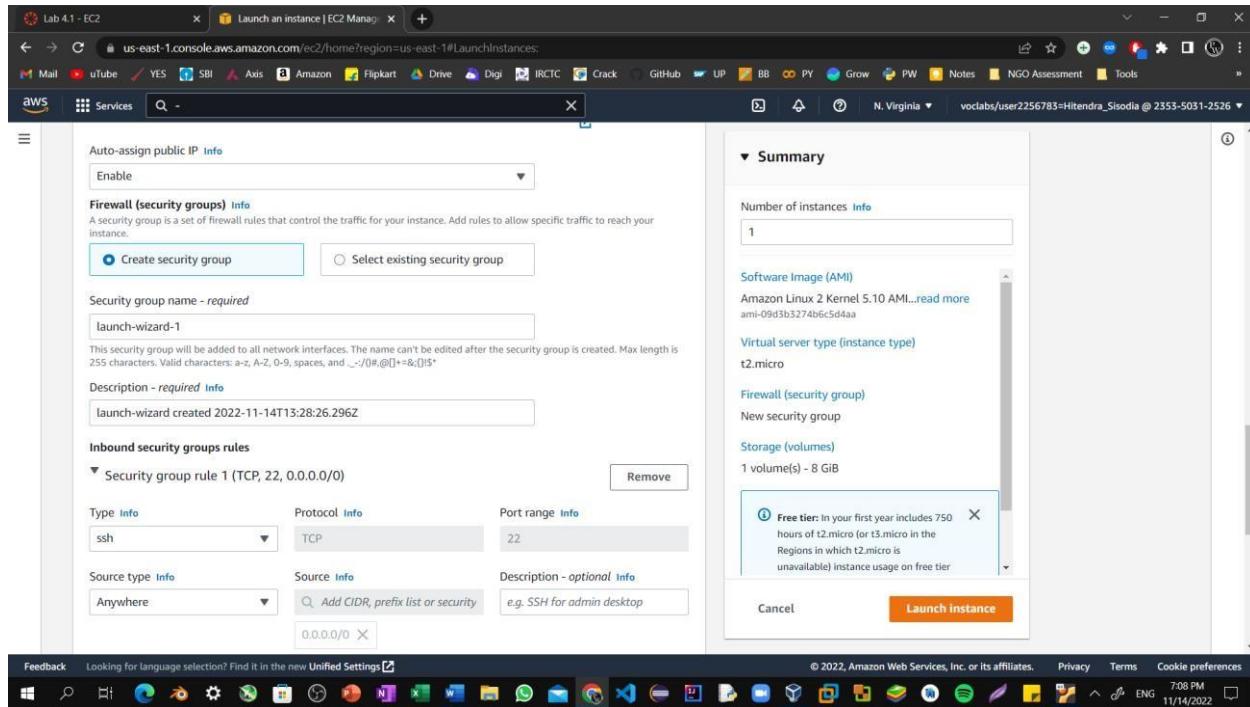


**Step8:** Next to Network settings, choose Edit. Keep the default VPC and subnet settings. Also keep the Auto-assign public IP setting set to Enable.

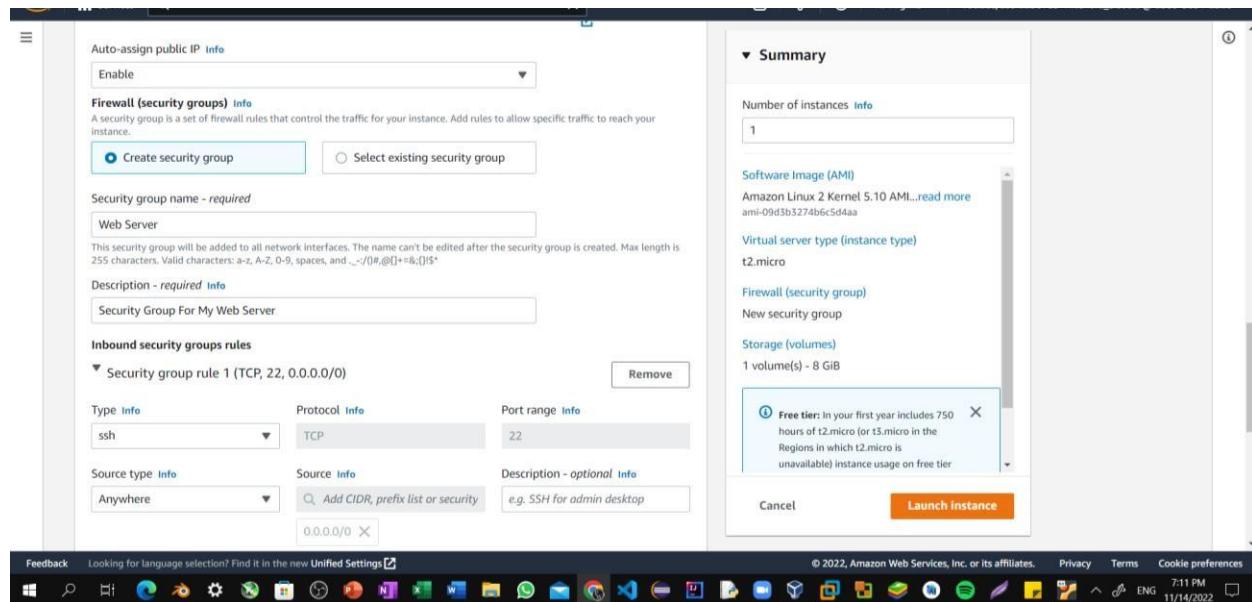


## Lab 10.1: Launching an EC2

Step9: Under Firewall (security groups), keep the default **Create security group** option chosen.

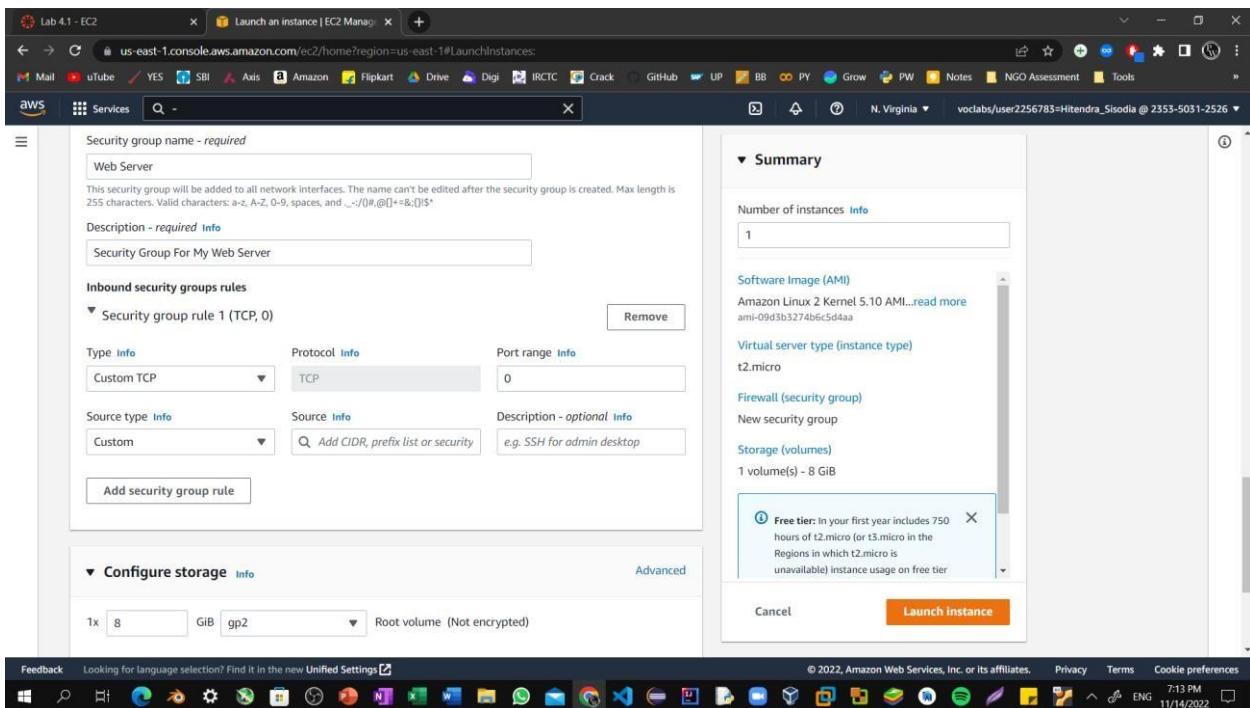


Step10: Configure a new security group:  
Keep the default selection **Create a new security group**.  
**Security group name:** Clear the text and enter Web Server.  
**Description:** Clear the text and enter Security group for my web server.

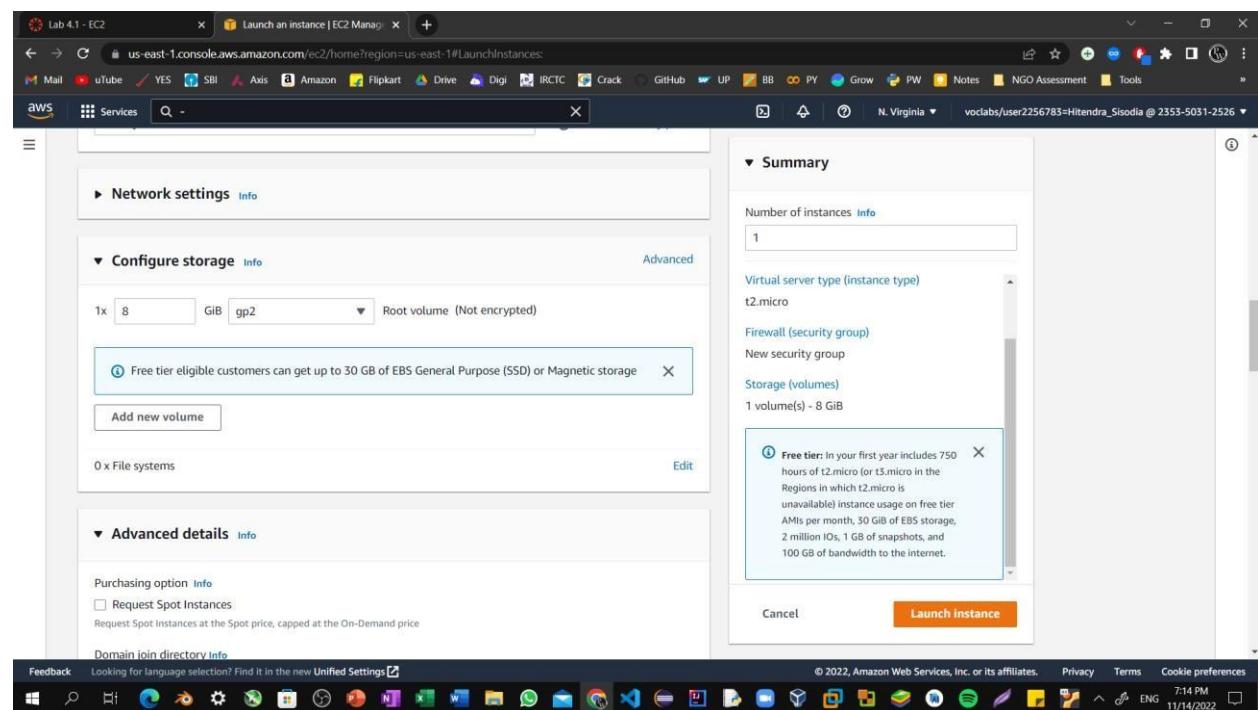


## Lab 10.1: Launching an EC2

Step11: Choose Remove to remove the default SSH inbound rule.



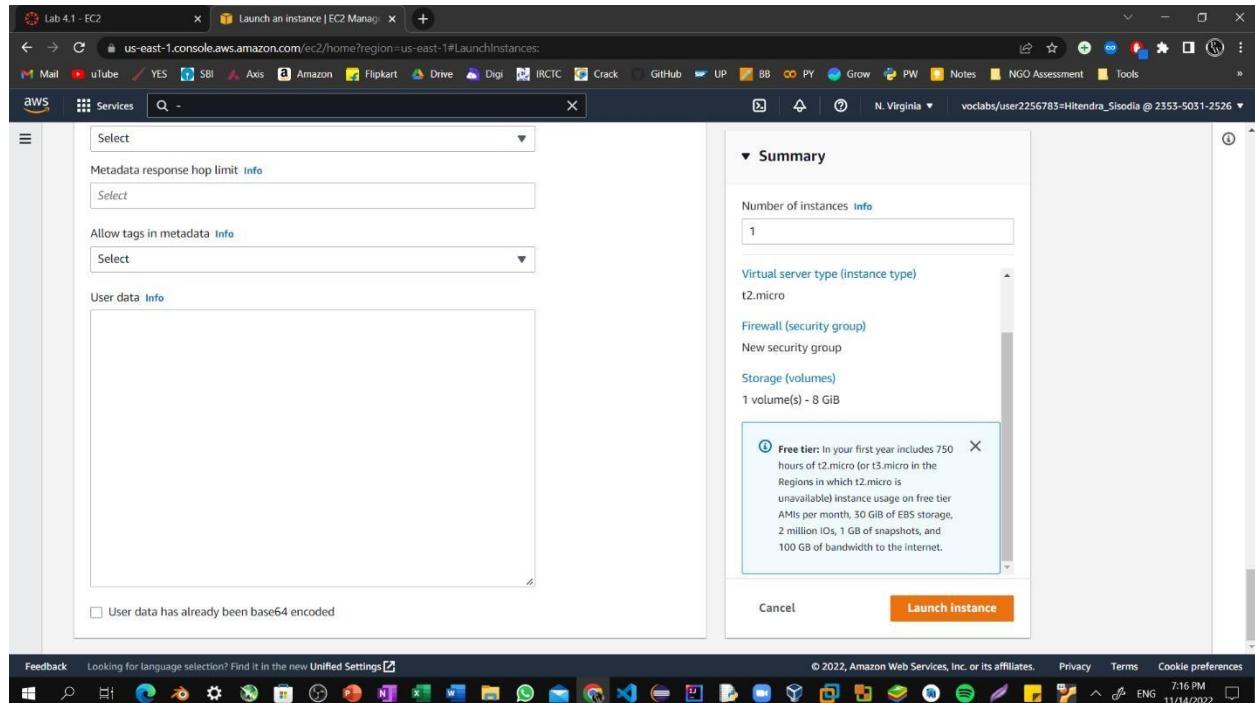
Step12: In the *Configure storage* section, keep the default settings. You will launch the Amazon EC2 instance using a default Elastic Block Store (EBS) disk volume.



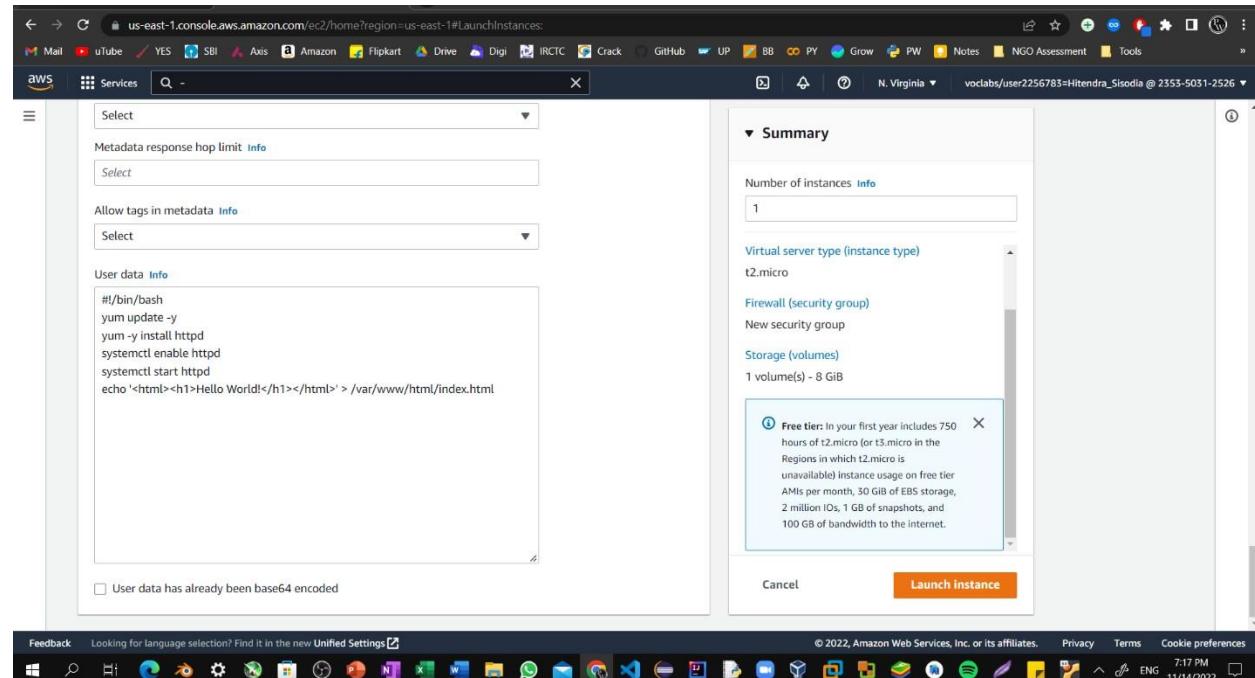
## Lab 10.1: Launching an EC2

Step13: Configure a script to run on the instance when it launches:

- Expand the **Advanced details** panel.

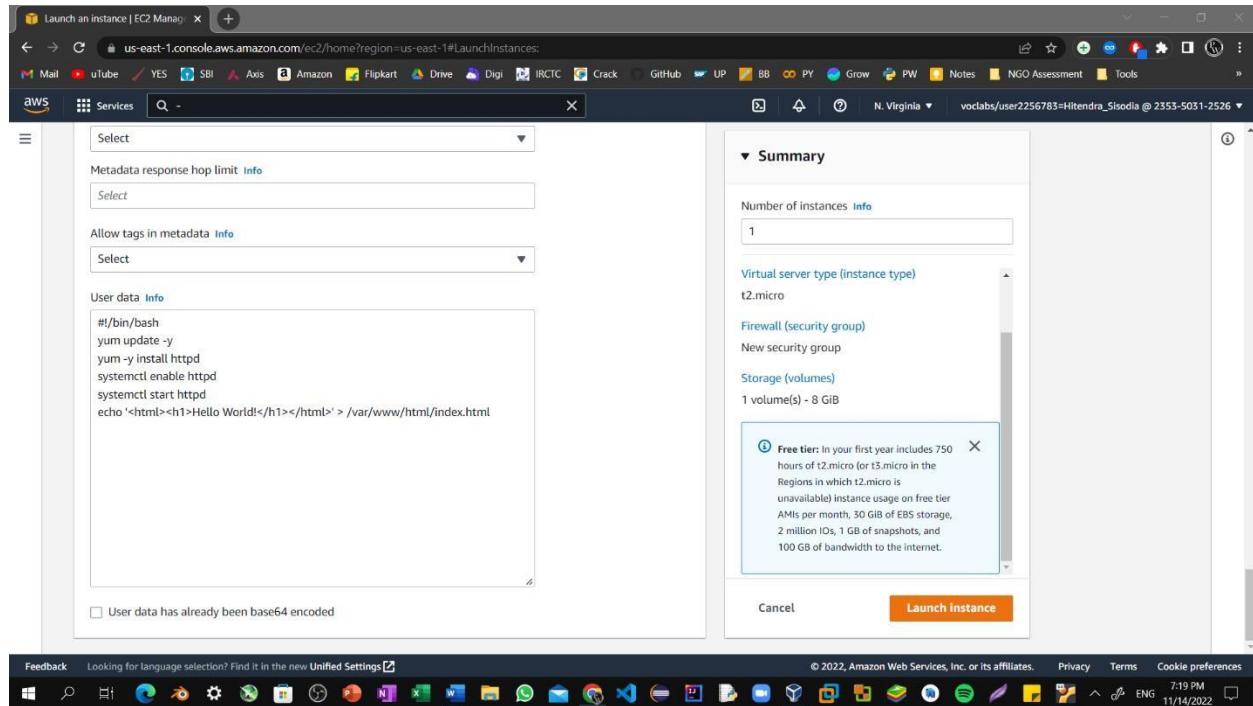


Step14: Scroll to the bottom of the page and then copy and paste the code shown below into the **User data** box.

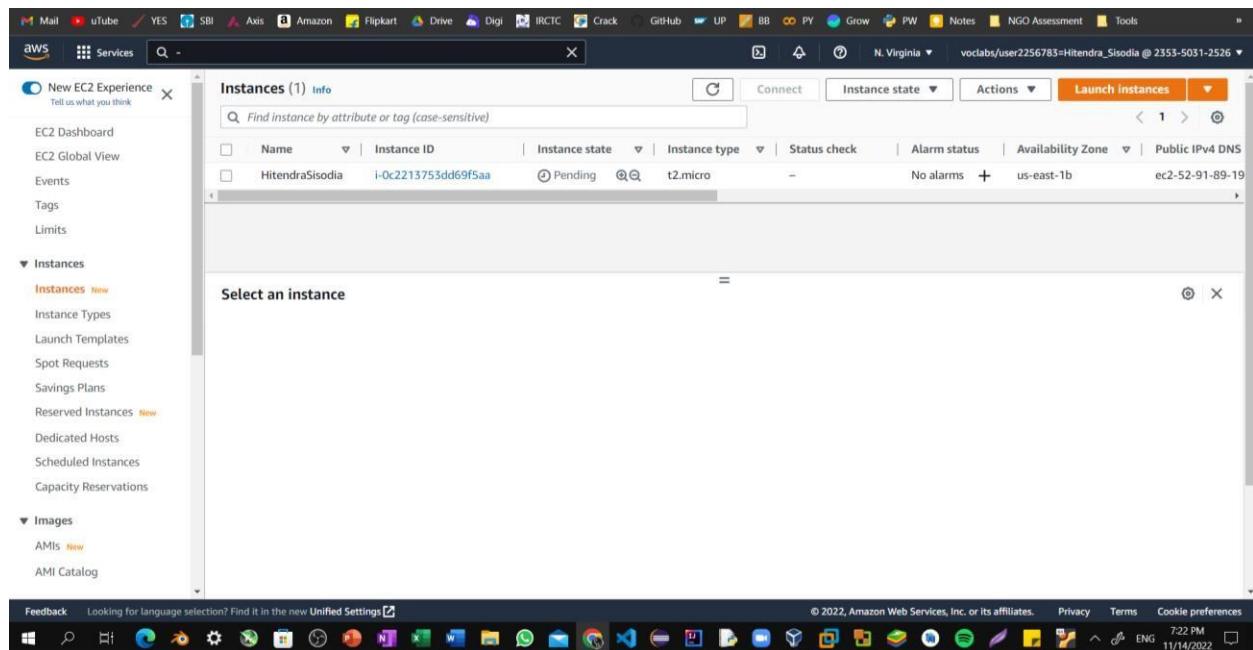


## Lab 10.1: Launching an EC2

Step15: At the bottom of the **Summary** panel on the right side of the screenchoose Launch Instances. You will see a Success message.

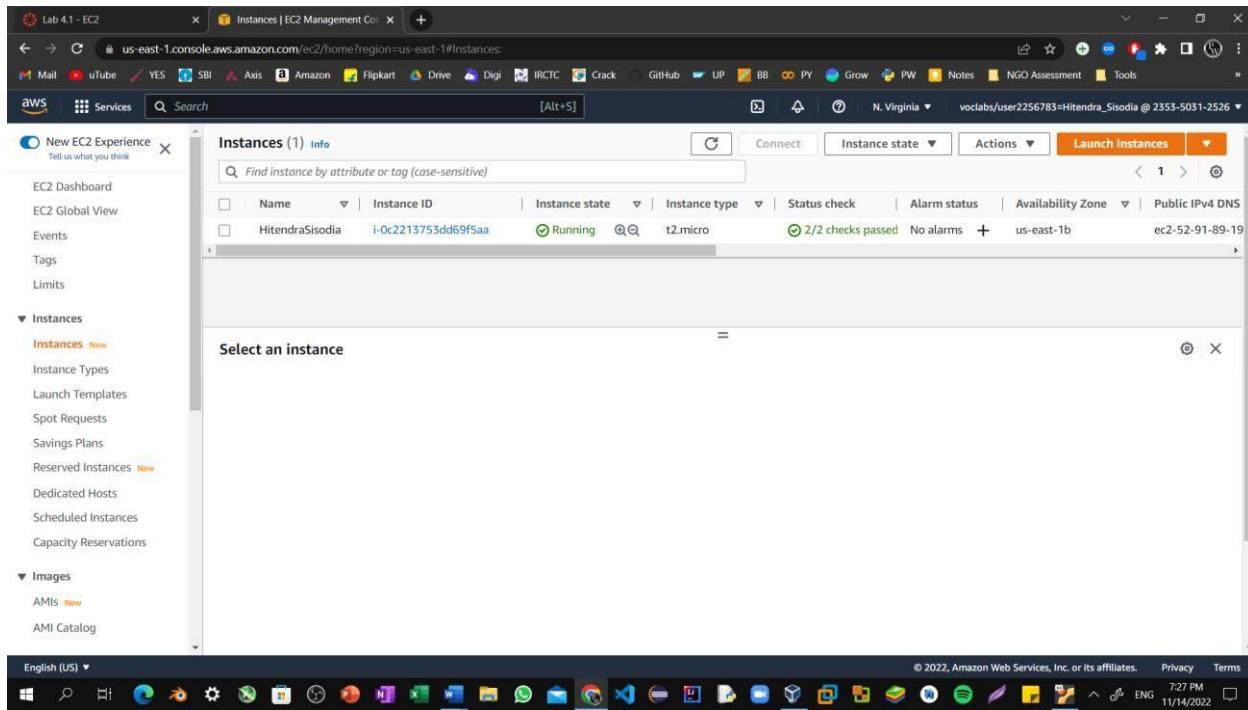


Step16: The instance will first appear in the *Pending* state, which means it is being launched. The state will then change to *Running*, which indicates that the instance has started booting. It takes a few minutes for the instance to boot.



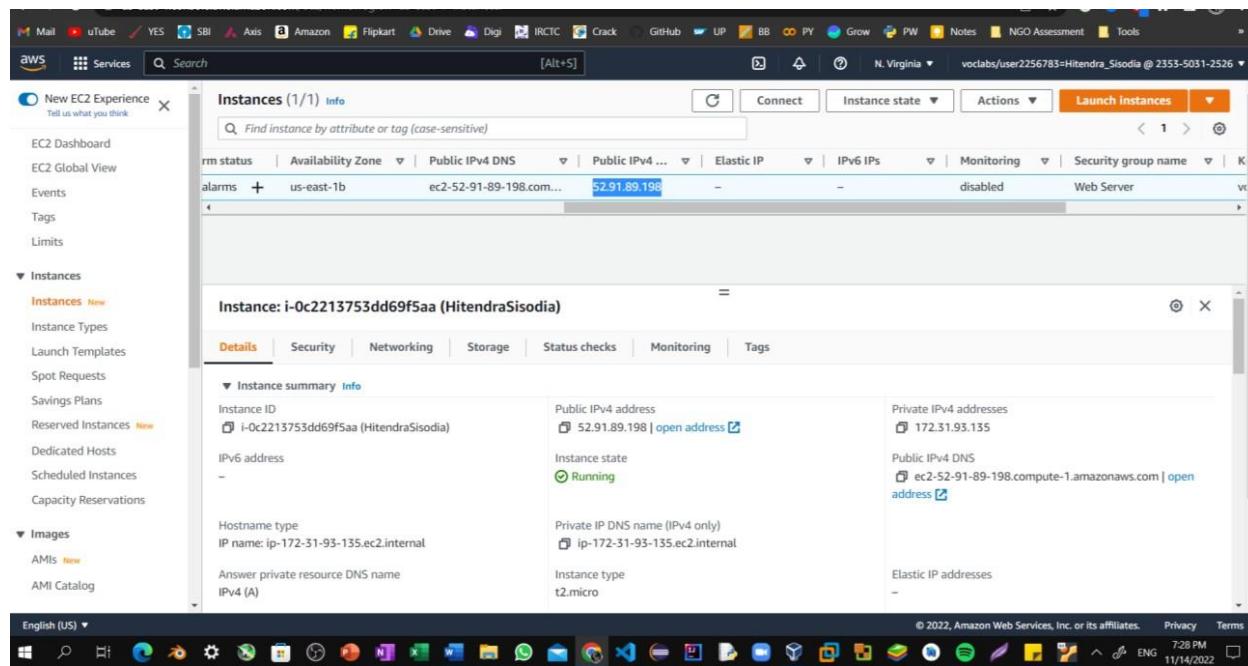
## Lab 10.1: Launching an EC2

**Step17:** Before you continue, wait for your instance to display the following:  
**Instance state:** Running  
**Status check:** 2/2 checks passed



The screenshot shows the AWS EC2 Instances Management Console. On the left, there's a sidebar with options like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, and Images. The main area displays a table titled 'Instances (1) Info'. It shows one instance: 'HitendraSisodia' (Instance ID: i-0c2213753dd69f5aa), which is 'Running' (Status check: 2/2 checks passed). Below the table, a modal window titled 'Select an instance' is open, showing the same instance. At the bottom, the Windows taskbar is visible with various pinned icons.

**Step18:** From the Details tab, copy the Public IPv4 address value of your instance to your clipboard.

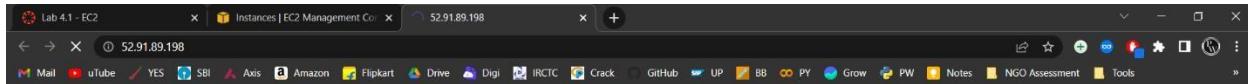


This screenshot shows the 'Details' tab for the instance 'i-0c2213753dd69f5aa' (HitendraSisodia). The table includes columns for Public IPv4 DNS, Elastic IP, IPv6 IPs, Monitoring, and Security group name. The Public IPv4 DNS is listed as 'ec2-52-91-89-198.com...'. The 'Details' tab itself has sections for Instance summary, Security, Networking, Storage, Status checks, Monitoring, and Tags. Under 'Instance summary', it shows the Instance ID (i-0c2213753dd69f5aa), Public IPv4 address (52.91.89.198), Private IPv4 addresses (172.31.93.155), Instance state (Running), Public IPv4 DNS (ec2-52-91-89-198.compute-1.amazonaws.com), Hostname type (IP name: ip-172-31-93-135.ec2.internal), Answer private resource DNS name (IPv4 (A)), and Instance type (t2.micro). The Windows taskbar is visible at the bottom.

## Lab 10.1: Launching an EC2

**Step19:** Open a new tab in your web browser, paste the public IP address you just copied, and press **Enter**.

The webpage does not load. You must update the security group to be able to access the page.



**Step20:** Return to the **EC2 Management Console** browser tab. In the left navigation pane, under **Network & Security**, choose **Security Groups**.

Name	Security group ID	VPC ID	Description	Owner
Web Server	sg-0628e6ae9e7e6ad67	vpc-03d6a9566a4951938	Security Group For My ...	235350312526
default	sg-00aaeceedad87b2b1	vpc-03d6a9566a4951938	default VPC security gr...	235350312526

## Lab 10.1: Launching an EC2

**Step21:** Select the **Web Server** security group, which you created when launching your EC2 instance. In the lower pane, choose the **Inbound rules** tab.

The screenshot shows the AWS EC2 Management Console. On the left, there's a navigation sidebar with options like AMIS, Elastic Block Store, Network & Security (Security Groups), Load Balancing, Auto Scaling, and Services. The main area displays a table of security groups. One row is selected, showing details: Name: Web Server, Security group ID: sg-0628e6ae9e7e6ad67, VPC ID: vpc-03d6a9566a4951938, Description: Security Group For My ..., Owner: 235350312526. Below the table, tabs for Details, Inbound rules, Outbound rules, and Tags are visible. The Inbound rules tab is selected, and a message says 'You can now check network connectivity with Reachability Analyzer'. A button to 'Run Reachability Analyzer' is present. At the bottom of the page, it says 'https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ModifyInboundSecurityGroupRules?securityGroupId=sg-0628e6ae9e7e6ad67'. The status bar at the bottom right shows the date and time: 7:34 PM 11/14/2022.

**Step22:** Choose **Edit inbound rules**, and then choose **Add rule**.

The screenshot shows the 'Edit inbound rules' page for the 'Web Server' security group. The URL is https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#ModifyInboundSecurityGroupRules?securityGroupId=sg-0628e6ae9e7e6ad67. The page has tabs for Inbound rules and Info. Under Inbound rules, there are columns for Security group rule ID, Type, Protocol, Port range, Source, and Description - optional. A 'Custom TCP' rule is listed with port 0 and source 'Custom'. Buttons for 'Delete' and 'Add rule' are present. At the bottom, there are 'Cancel', 'Preview changes', and 'Save rules' buttons. The status bar at the bottom right shows the date and time: 7:34 PM 11/14/2022.

## Lab 10.1: Launching an EC2

**Step23: Configure the following:**

**Type:** HTTP

**Source:** Anywhere-IPv4 Choose Save rules

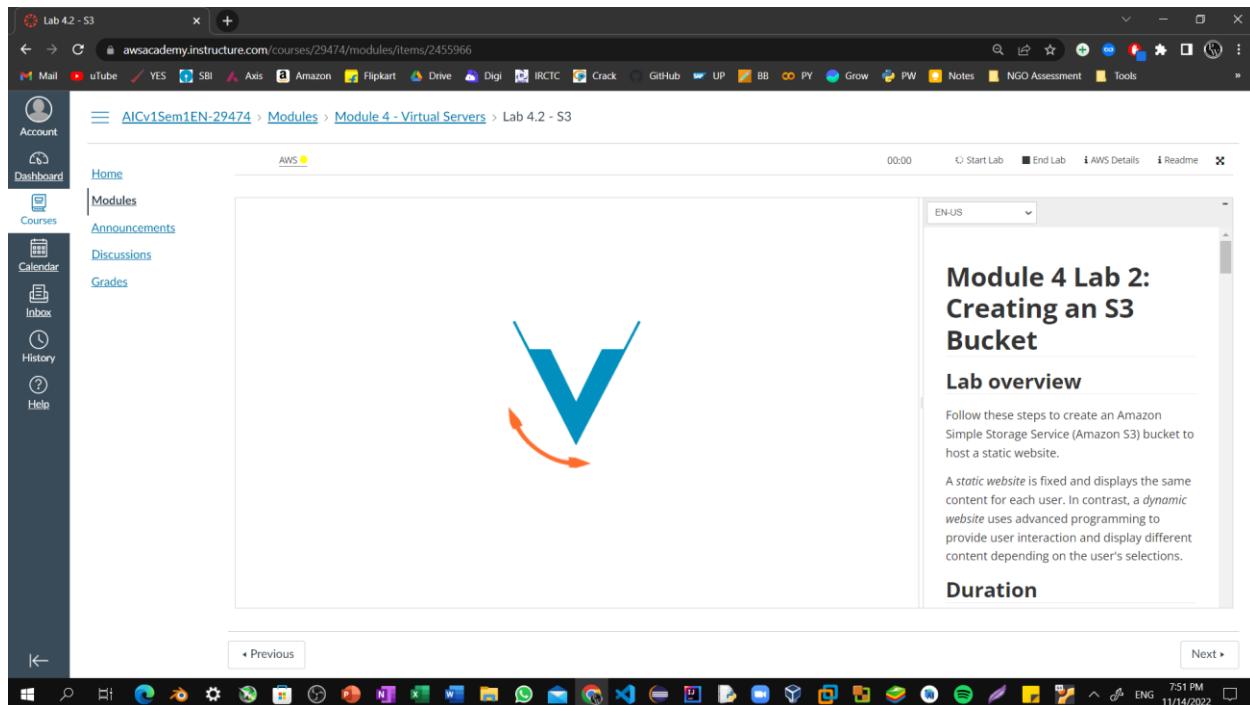
The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with options like EC2 Dashboard, EC2 Global View, Events, Tags, Instances (with sub-options like Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations), Images (AMIs, AMI Catalog), and English (US). The main area shows a success message: "Inbound security group rules successfully modified on security group (sg-0628e6ae9e7e6ad67 | Web Server) Details". Below this is a table titled "Security Groups (1/2)" with one row. The row has a checkbox (unchecked), Name (sg-00aeecedad87b2b1), Security group ID (sg-00aeecedad87b2b1), Security group name (default), VPC ID (vpc-03d6a9566a4951938), Description (default VPC security gr...), and Owner (235350312526). A second row is selected, showing a checked checkbox, Name (sg-0628e6ae9e7e6ad67), Security group ID (sg-0628e6ae9e7e6ad67), Security group name (Web Server), VPC ID (vpc-03d6a9566a4951938), Description (Security Group For My ...), and Owner (235350312526). Below the table, it says "sg-0628e6ae9e7e6ad67 - Web Server". Under "Inbound rules", there's a note: "You can now check network connectivity with Reachability Analyzer" with a "Run Reachability Analyzer" button. At the bottom right of the main window, there's a footer with "© 2022, Amazon Web Services, Inc. or its affiliates.", "Privacy", and "Terms". The taskbar at the bottom of the screen shows various icons for different applications.

**Step24: Return to the tab that you used to try to connect to the web server.  
The page should display the message *Hitendra Sisodia*.**

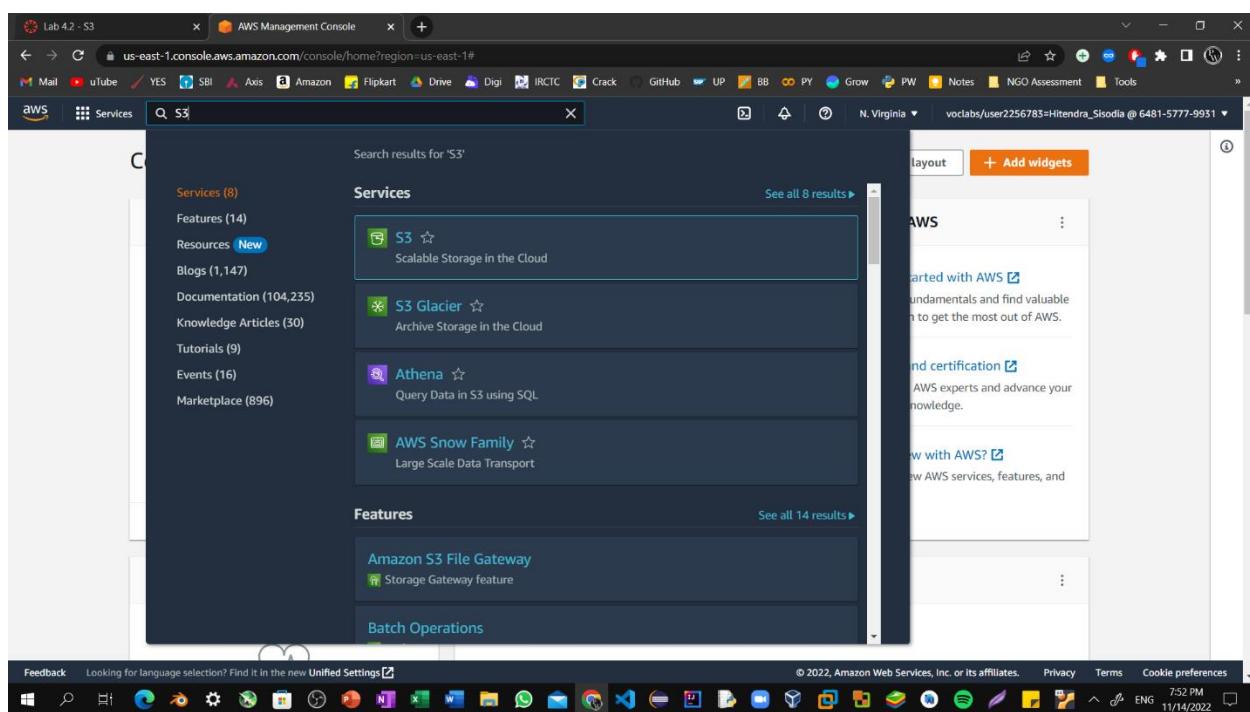
The screenshot shows a browser window with the URL "Not secure | 52.91.89.198". The main content area displays the text "Hitendra Sisodia". The browser toolbar at the top includes icons for Back, Forward, Stop, Refresh, Home, and various tabs. The taskbar at the bottom of the screen shows various application icons.

## Lab 10.2: Launching an S3 Bucket

Step1: To start the lab session, choose **Start Lab** in the upper-right corner of the page.



Step2: Choose the **Services** menu, locate the **Storage** services, and select **S3**.



## Lab 10.2: Launching an S3 Bucket

Step3: Select Create bucket on the right side of the page.

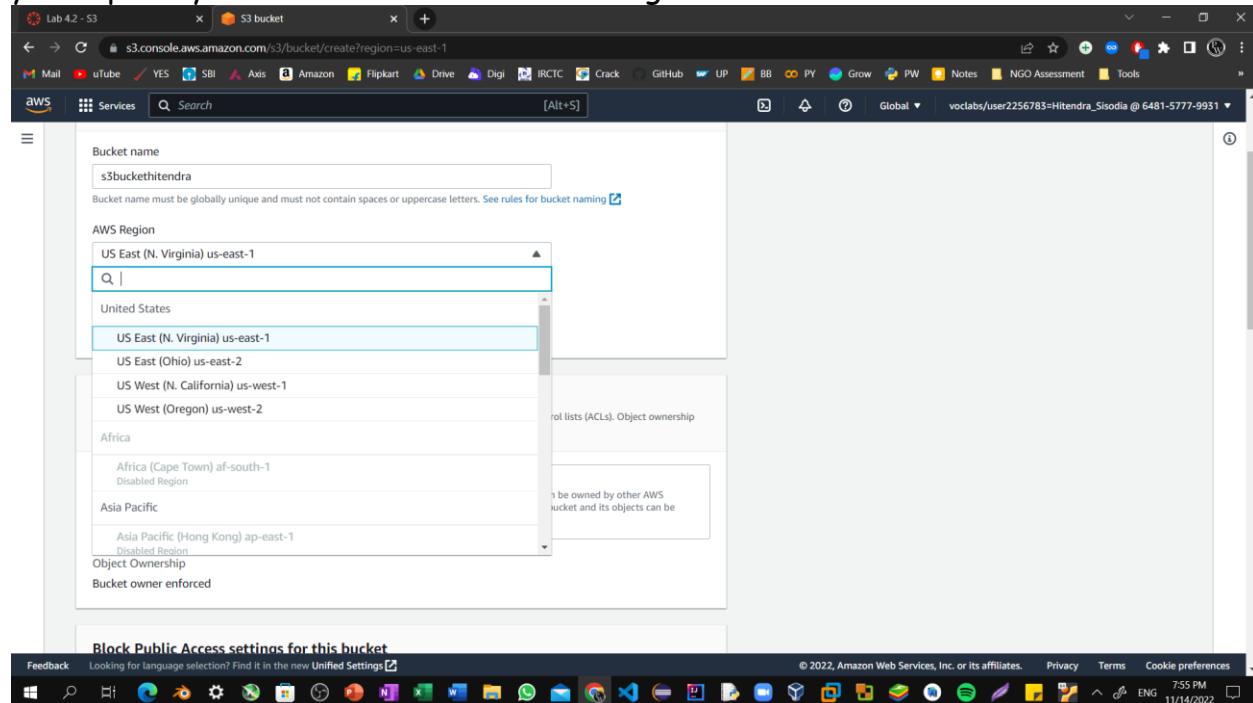
The screenshot shows the AWS S3 Management Console. On the left, there's a sidebar with 'Storage' and 'Amazon S3'. The main area has a heading 'Amazon S3' and sub-headings 'Store and retrieve any amount of data from anywhere' and 'How it works'. On the right, a 'Create a bucket' dialog box is open, containing text about object storage and a 'Create bucket' button. Below the dialog, there are sections for 'Pricing' and 'Resources'. The browser address bar shows 's3.console.aws.amazon.com/s3/get-started?region=us-east-1'. The taskbar at the bottom includes icons for various Windows applications like Mail, YouTube, and File Explorer.

Step4: For Bucket name, enter a unique Domain Name System (DNS)-compliant name for your new bucket.

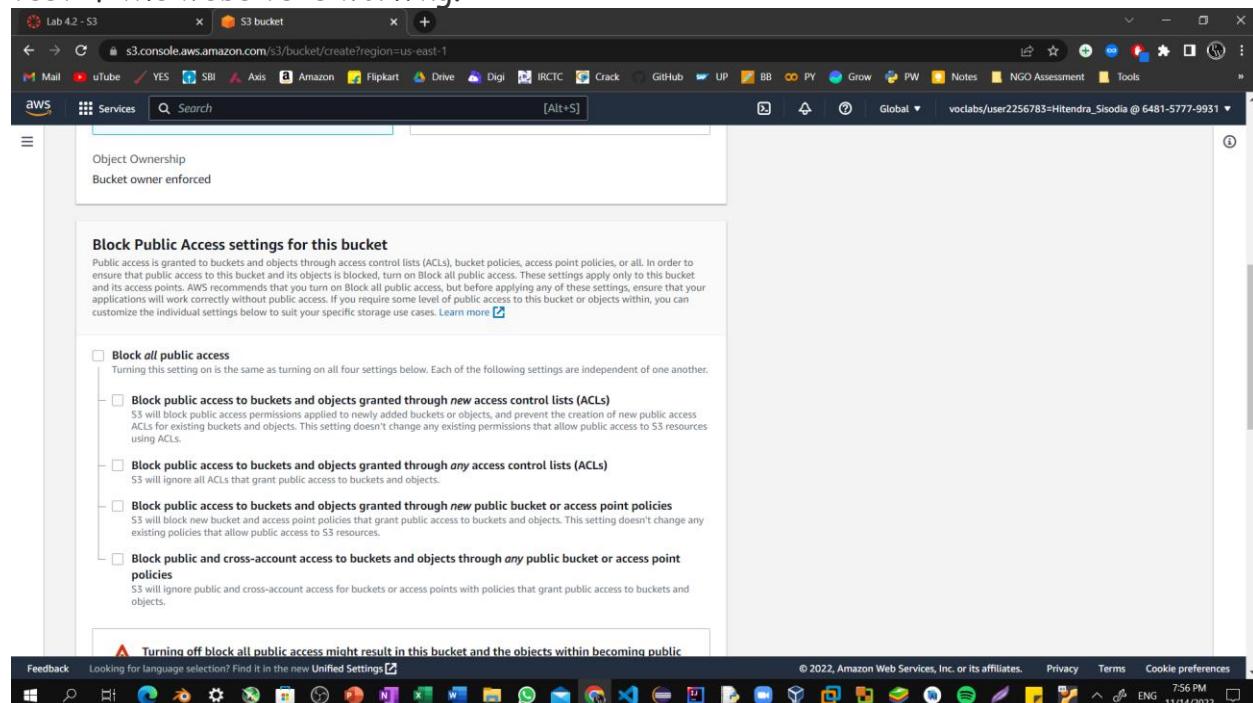
The screenshot shows the 'Create bucket' configuration page. The 'General configuration' section is visible, with the 'Bucket name' field set to 's3buckethitendra'. The 'AWS Region' dropdown is set to 'US East (N. Virginia) us-east-1'. Below this, there's a 'Copy settings from existing bucket - optional' section with a 'Choose bucket' button. The 'Object Ownership' section shows 'ACLs disabled (recommended)'. The browser address bar shows 's3.console.aws.amazon.com/s3/bucket/create?region=us-east-1'. The taskbar at the bottom includes icons for various Windows applications like Mail, YouTube, and File Explorer.

## Lab 10.2: Launching an S3 Bucket

**Step5: For Region, choose the AWS Region where you want the bucket to reside. Choose a Region close to you to minimize latency and costs, or to address regulatory requirements. Objects stored in a Region never leave that Region unless you explicitly transfer them to another Region.**

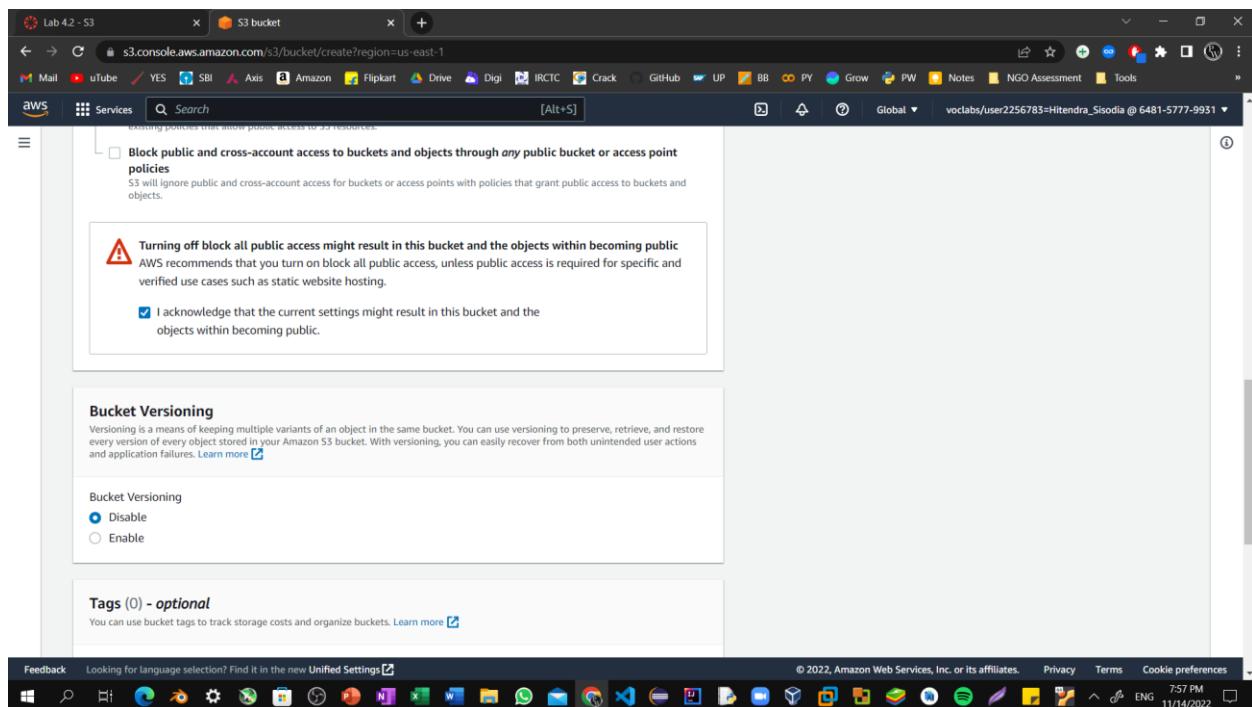


**Step6: Uncheck the Block all public access box because you want to be able to test if the website is working.**

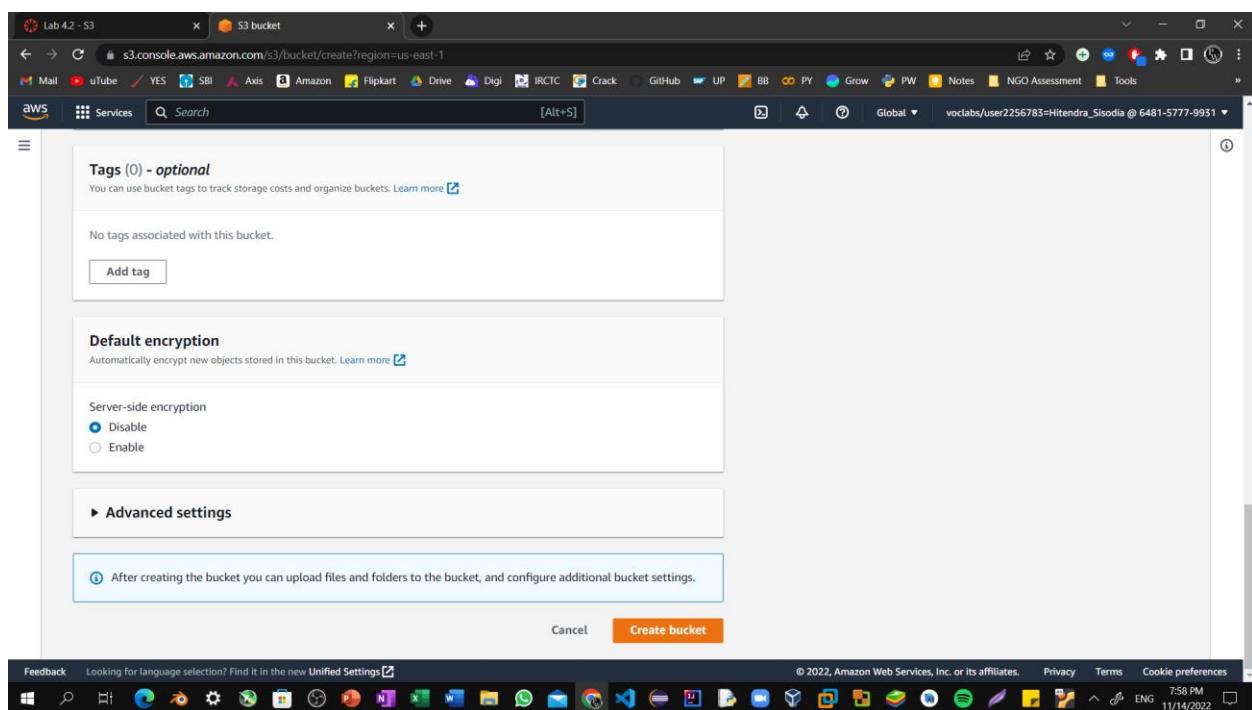


## Lab 10.2: Launching an S3 Bucket

Step7: Below the warning, check the box next to I acknowledge that....



Step8: Scroll to the bottom of the page, and select Create bucket.



## Lab 10.2: Launching an S3 Bucket

Step9: Successfully created Bucket.

The screenshot shows the AWS S3 Management Console. A green banner at the top indicates that a bucket named "s3buckethitendra" has been successfully created. Below the banner, the "Buckets" section displays one item: "s3buckethitendra" from the "us-east-1" region. The object is public and was created on November 14, 2022. On the left sidebar, the "Buckets" section is expanded, showing various options like Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and Access analyzer for S3. The status bar at the bottom shows the date and time as 11/14/2022 8:00 PM.

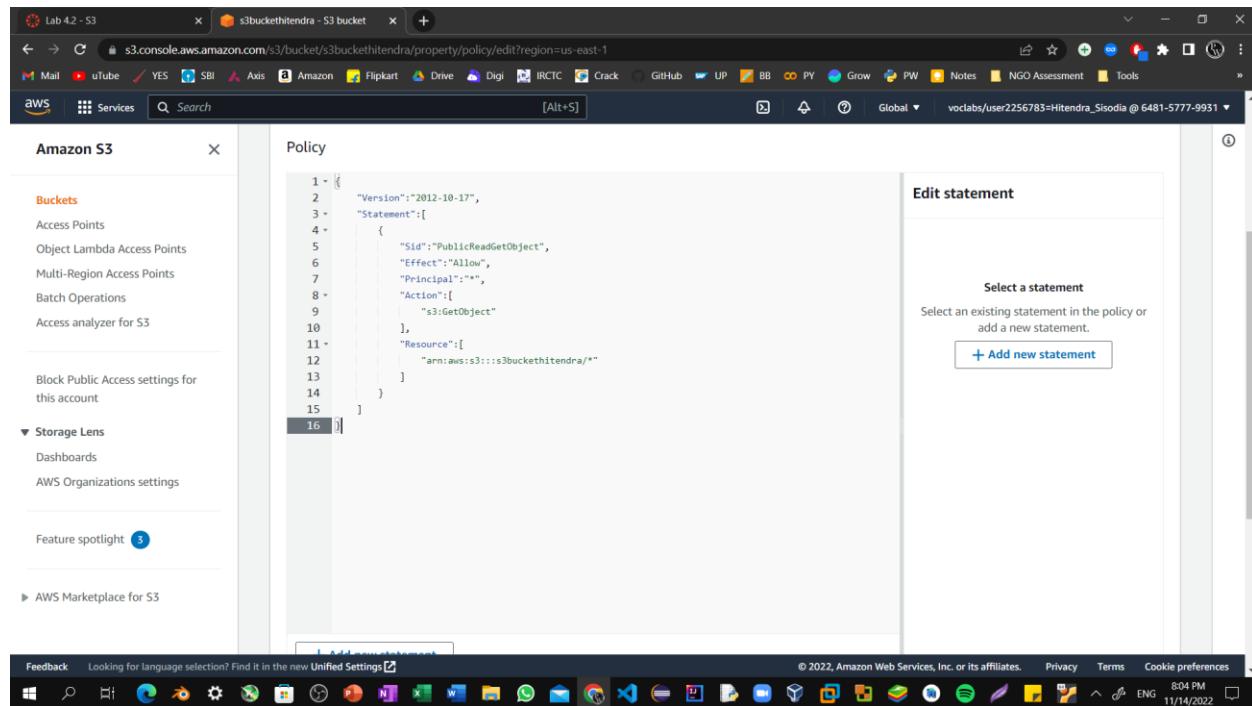
Step10: Choose the link for your bucket's name, and then select the permission tab.

The screenshot shows the AWS S3 Management Console for the "s3buckethitendra" bucket. The "Permissions" tab is selected in the navigation bar. Under the "Permissions overview" section, it states that objects can be public. In the "Block public access (bucket settings)" section, it says "Block all public access" is off. The status bar at the bottom shows the date and time as 11/14/2022 8:02 PM.

## Lab 10.2: Launching an S3 Bucket

Step11: In the Bucket policy section, choose Edit.

To grant public read access for your website, copy the following bucket policy, and paste it in the policy editor.

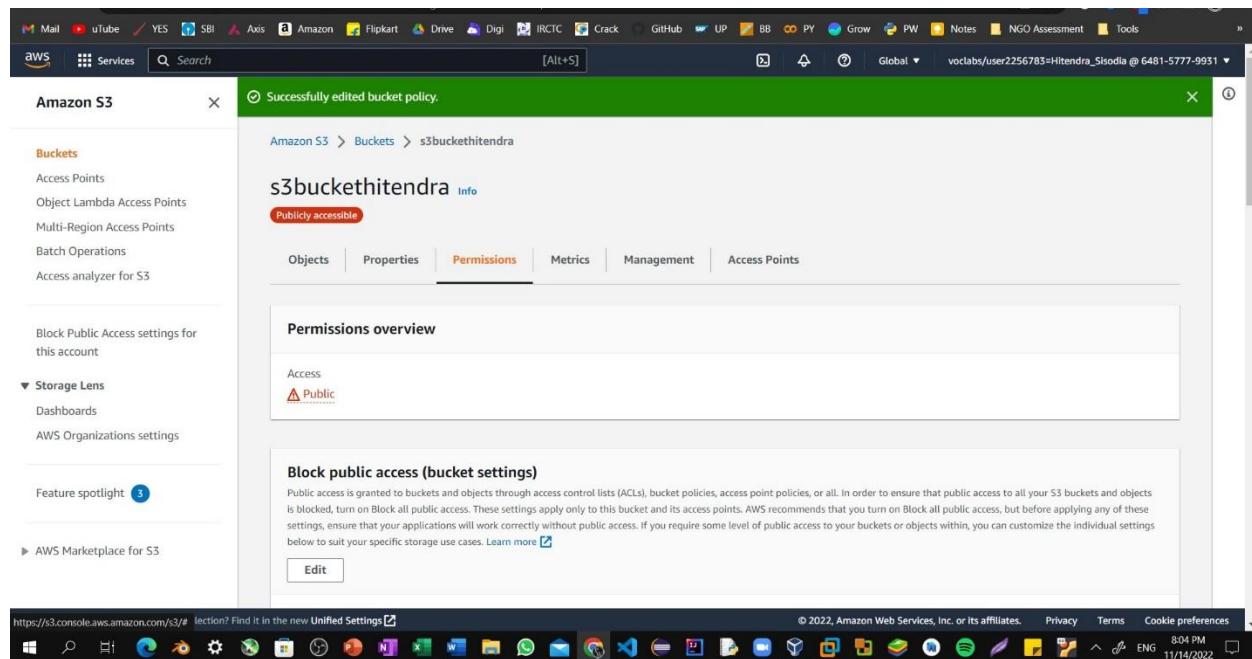


The screenshot shows the AWS S3 console with the 'Edit statement' dialog open. The policy JSON is displayed:

```
1 ~ {
2     "Version": "2012-10-17",
3     "Statement": [
4         {
5             "Sid": "PublicReadGetObject",
6             "Effect": "Allow",
7             "Principal": "*",
8             "Action": [
9                 "s3:GetObject"
10            ],
11            "Resource": [
12                "arn:aws:s3:::s3buckethitendra/*"
13            ]
14        }
15    ]
16 }
```

The 'Edit statement' dialog has a placeholder 'Select a statement' and a button '+ Add new statement'.

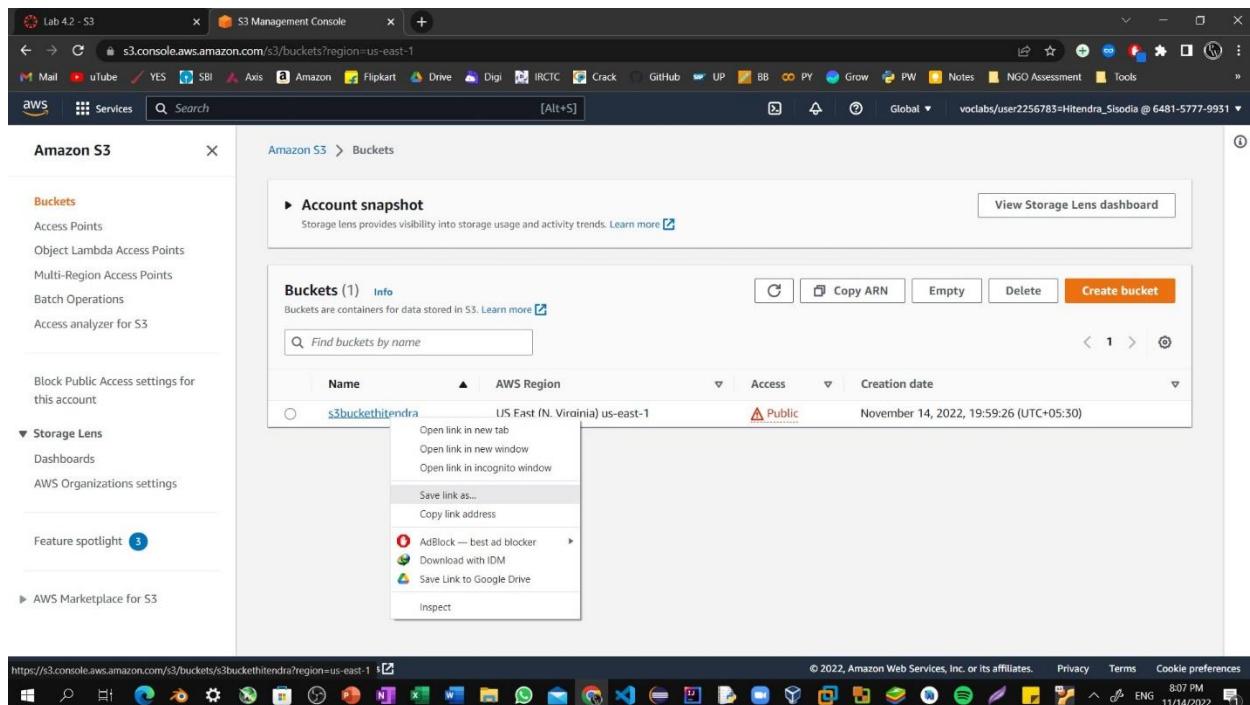
Step12: In the policy, replace **example-bucket** with the name of your bucket.  
Select **Save changes**.



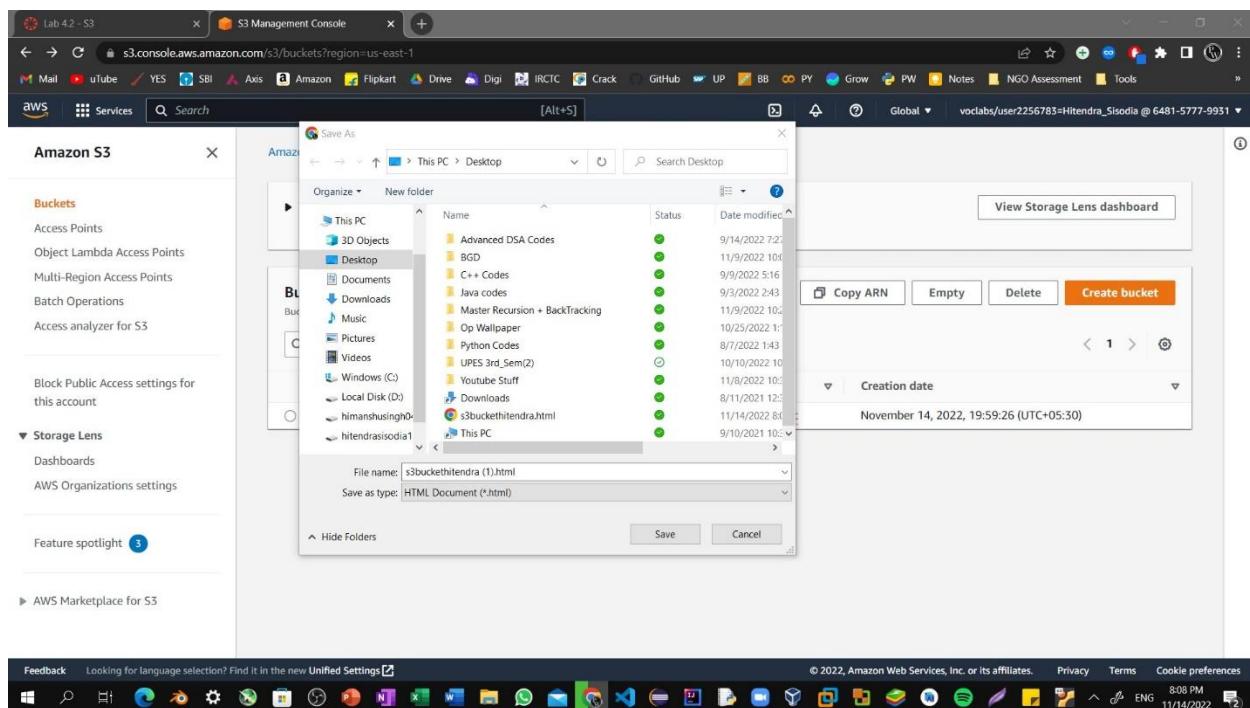
The screenshot shows the 'Permissions' tab of the S3 bucket configuration. A green success message 'Successfully edited bucket policy.' is displayed. The 'Permissions overview' section shows 'Access Public'. The 'Block public access (bucket settings)' section contains a note about enabling public access through various methods like ACLs or bucket policies, with a link to learn more.

## Lab 10.2: Launching an S3 Bucket

Step13: Open the context menu (right-click) for the following link, and then choose **Save link as: index.html**



Step14: Save the index.html file to your local computer.



## Lab 10.2: Launching an S3 Bucket

Step15: In the console, choose the **Objects** tab.

The screenshot shows the AWS S3 console with the URL [s3.console.aws.amazon.com/s3/buckets/s3buckethitendra?region=us-east-1&tab=objects](https://s3.console.aws.amazon.com/s3/buckets/s3buckethitendra?region=us-east-1&tab=objects). The left sidebar is collapsed. The main area shows the 'Objects' tab selected under the 's3buckethitendra' bucket. A message states 'Objects (0)' and 'No objects'. Below this, there is a search bar and a large orange 'Upload' button. The top navigation bar includes tabs for 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The status bar at the bottom shows the date and time as '11/14/2022 8:11 PM'.

Step16: Upload the index.html file to your bucket.

Choose **Upload**.

Drag and drop the index.html file onto the upload page.

As an alternative, choose **Add files**, navigate to the file, and choose **Open**.

The screenshot shows the AWS S3 console with the URL [s3.console.aws.amazon.com/s3/buckets/s3buckethitendra/Upload](https://s3.console.aws.amazon.com/s3/buckets/s3buckethitendra/Upload). The left sidebar is collapsed. The main area shows the 'Upload' tab selected. A message says 'Add the files and folders you want to upload to S3.' Below is a large dashed box for dragging files. A table lists 'Files and folders (1 Total, 426.9 KB)' with one entry: 's3buckethitendra.html'. Under 'Destination', it shows 's3://s3buckethitendra'. The status bar at the bottom shows the date and time as '11/14/2022 8:13 PM'.

## Lab 10.2: Launching an S3 Bucket

Step17: Expand the Permissions section.

The screenshot shows the AWS S3 Management Console interface. In the 'Destination' section, the 'Destination' field is set to 's3://s3buckethitendra'. Below it, the 'Destination details' section is expanded, showing 'Bucket settings that impact new objects stored in the specified destination.' In the 'Permissions' section, which is also expanded, there is a note: 'This bucket has the bucket owner enforced setting applied for Object Ownership. Use bucket policies to control access.' The 'Properties' section is partially visible at the bottom. The browser's address bar shows the URL 's3.console.aws.amazon.com/s3/upload/s3buckethitendra?region=us-east-1'. The taskbar at the bottom includes icons for various applications like Mail, YouTube, and Google Chrome.

Step18: Under Predefined ACLs, select Grant public-read access. A warning message similar to **Granting public-read access is not recommended** appears below the setting you selected.

The screenshot shows the 'Access control list (ACL)' configuration page. The 'Choose from predefined ACLs' option is selected, and 'Grant public-read access' is chosen. A warning message 'Granting public-read access is not recommended' is displayed, stating 'Anyone in the world will be able to access the specified objects.' Below this message is a checkbox labeled 'I understand the risk of granting public-read access to the specified objects.' The 'Properties' section is partially visible at the bottom. The browser's address bar shows the URL 's3.console.aws.amazon.com/s3/upload/s3hitendra?region=us-east-1'. The taskbar at the bottom includes icons for various applications like Mail, YouTube, and Google Chrome.

## Lab 10.2: Launching an S3 Bucket

Step19: Expand the **Properties** section. Ensure that the **Standard** storage class is selected.

The screenshot shows the AWS S3 Management Console with a new bucket named 's3buckethitendra' being created. In the 'Properties' section, the 'Storage class' dropdown is expanded, showing various options: Standard, Intelligent-Tiering, Standard-IA, One Zone-IA, Glacier Instant Retrieval, Glacier Flexible Retrieval, and Amazon S3 Standard-Infrequent Access (S3 IA). The 'Standard' option is selected, indicated by a blue circle with a dot. The table provides details for each class, such as designed for, availability zones, and min storage duration.

Step20: At the bottom of the page, choose **Upload**.

The screenshot shows the final configuration steps before uploading. It includes sections for 'Additional checksums' (Off), 'Tags - optional' (No tags associated), and 'Metadata - optional' (No metadata associated). At the bottom, there are 'Cancel' and 'Upload' buttons, with 'Upload' being the active one.

## Lab 10.2: Launching an S3 Bucket

Step21: Choose **Close**. The index.html file appears in the **Objects** list.

The screenshot shows the AWS S3 Management Console in a browser window. The title bar says "Lab 4.2 - S3" and "S3 Management Console". The address bar shows "s3.console.aws.amazon.com/s3/upload/s3buckethitendra?region=us-east-1". The main content area displays an "Upload succeeded" message with a link to "View details below." Below this, there's a summary table:

Destination	Succeeded	Failed
s3://s3buckethitendra	1 file, 426.9 KB (100.00%)	0 files, 0 B (0%)

Below the summary, there are tabs for "Files and folders" (which is selected) and "Configuration". Under "Files and folders", there's a table showing the uploaded file:

Name	Type	Size	Status
index.html	text/html	426.9 KB	Succeeded

At the bottom of the page, there's a note about language selection and links for "Feedback", "Privacy", "Terms", and "Cookie preferences". The status bar at the bottom of the browser shows "ENG 8:19 PM 11/14/2022".

Step22: Select the **Properties** tab, and scroll down to the **Static website hosting** section. Choose Edit, Select Enable

The screenshot shows the AWS S3 Properties page for the bucket "s3buckethitendra". The title bar says "Lab 4.2 - S3" and "s3buckethitendra - S3 bucket". The address bar shows "s3.console.aws.amazon.com/s3/bucket/s3buckethitendra/property/website/edit?region=us-east-1". The main content area shows the "Edit static website hosting" section:

**Static website hosting**  
Use this bucket to host a website or redirect requests. [Learn more](#)

**Static website hosting**  
 Enable  
 Disable

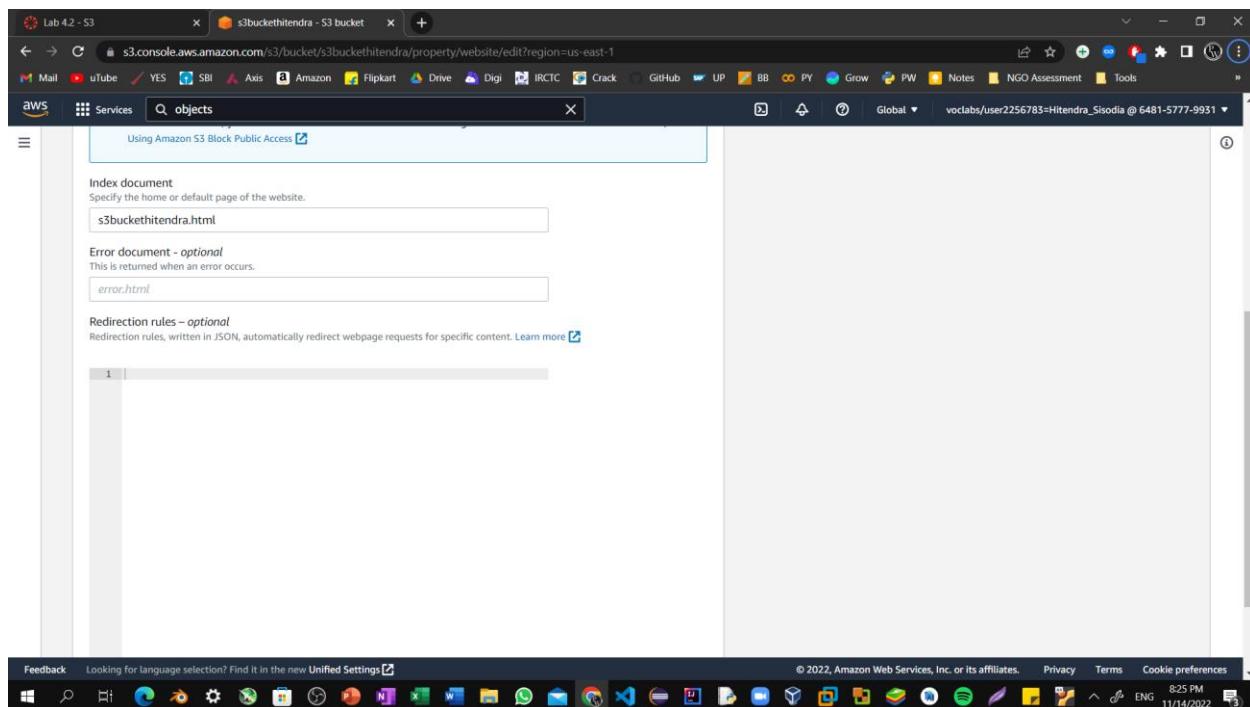
**Hosting type**  
 Host a static website  
Use the bucket endpoint as the web address. [Learn more](#)  
 Redirect requests for an object  
Redirect requests to another bucket or domain. [Learn more](#)

**Index document**  
Specify the home or default page of the website.

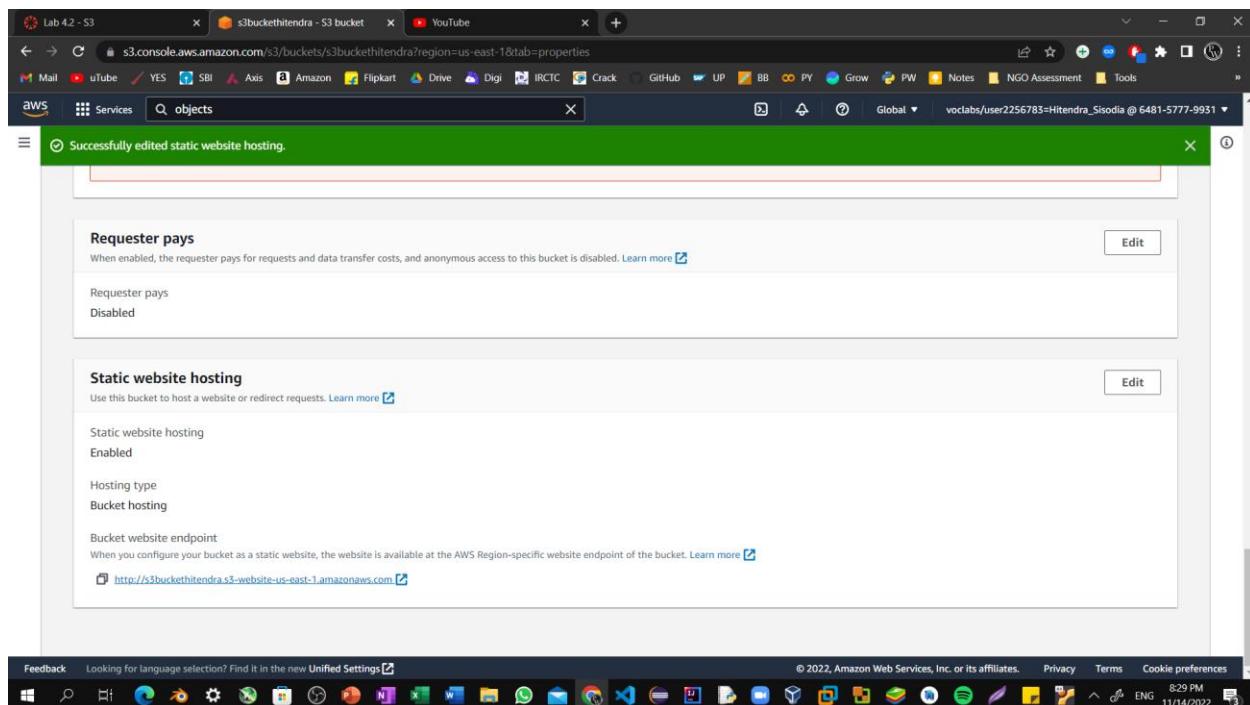
At the bottom, there's a note about making content publicly readable via S3 Block Public Access, a "Feedback" link, and links for "Privacy", "Terms", and "Cookie preferences". The status bar at the bottom of the browser shows "ENG 8:23 PM 11/14/2022".

## Lab 10.2: Launching an S3 Bucket

**Step23:** In the **Index document** text box, enter bucket-name.html Select **Save changes**.

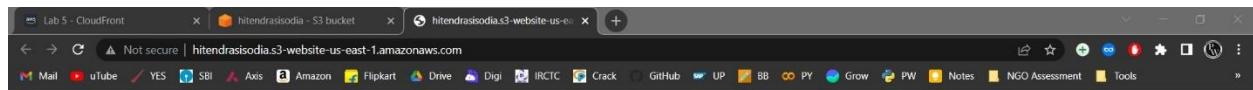


**Step24:** Scroll down to the **Static website hosting** section again, and copy the **Bucket website endpoint URL** to your clipboard.



## Lab 10.2: Launching an S3 Bucket

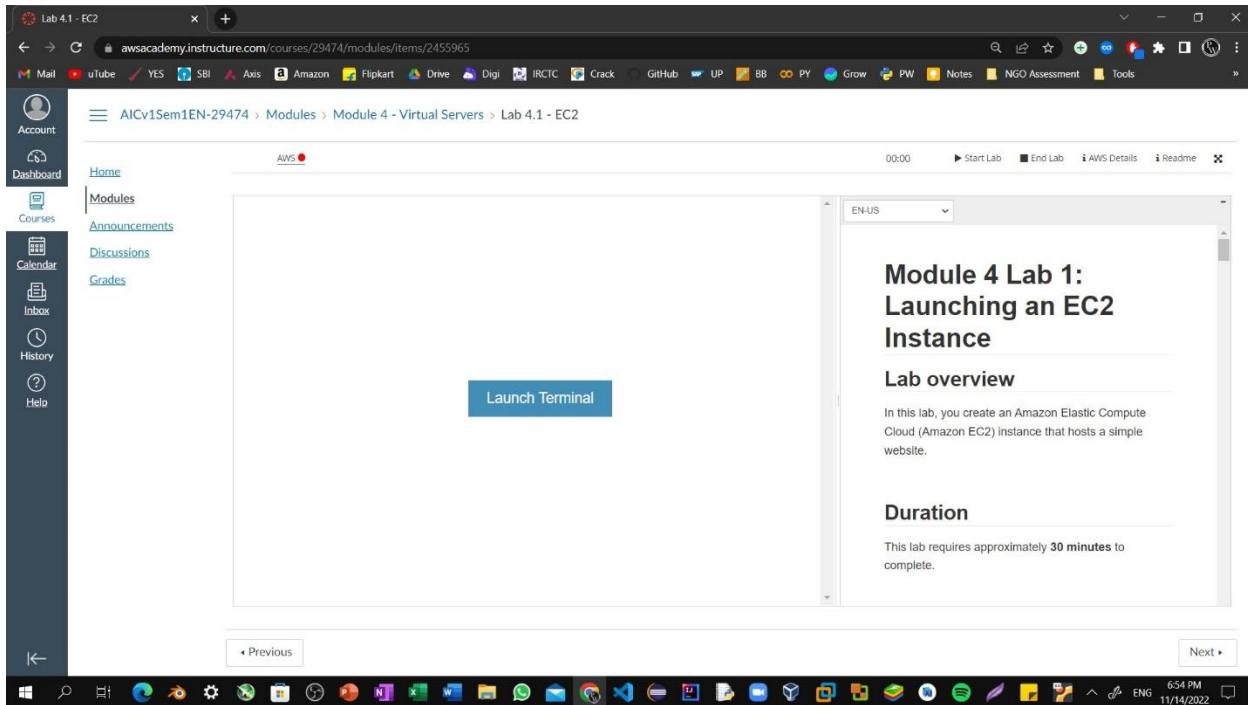
Step24: Static hosted website with EBS storage.



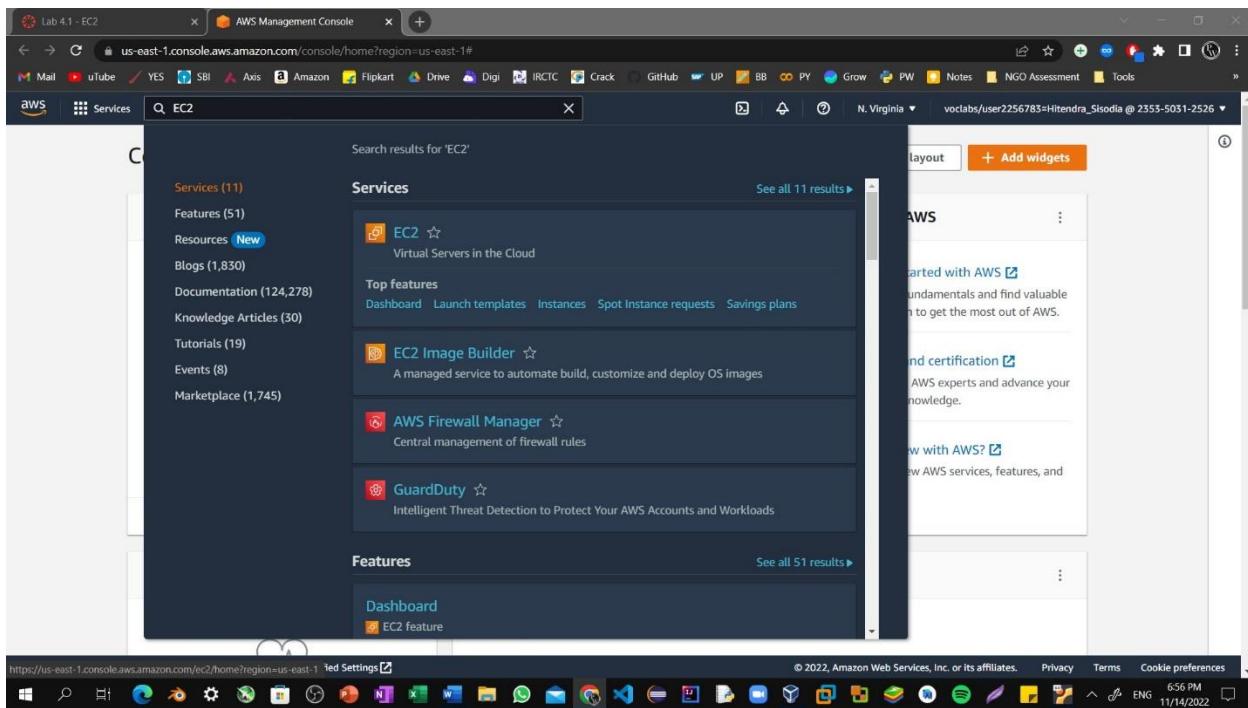
Hello World. Take me to your leader.

## Lab 11: Launching an EC2 Instance With EBS Storage

Step1: To start the lab session, choose **Start Lab** in the upper-right corner of the page.



Step2: Choose the **Services** menu, locate the **Compute** services, and select **EC2**.



## Lab 11: Launching an EC2 Instance With EBS Storage

Step3: Choose the **Launch instance** button in the middle of the page, and then select **Launch instance** from the dropdown menu.

The screenshot shows the AWS EC2 Dashboard. On the left sidebar, under 'Instances', 'Instances New' is selected. In the main content area, there is a 'Launch instance' section with a large orange 'Launch instance' button. To the right, there's a 'Service health' section showing 'US East (N. Virginia)' is operating normally, and a 'Zones' table listing four availability zones: us-east-1a, us-east-1b, us-east-1c, and us-east-1d, each associated with zone ID use1-az1 through use1-az6 respectively. On the far right, there's an 'Explore AWS' sidebar with various links like '10 Things You Can Do Today to Reduce AWS Costs' and 'Amazon GuardDuty Malware Protection'.

Step4: Name the instance: HitendraSisodia

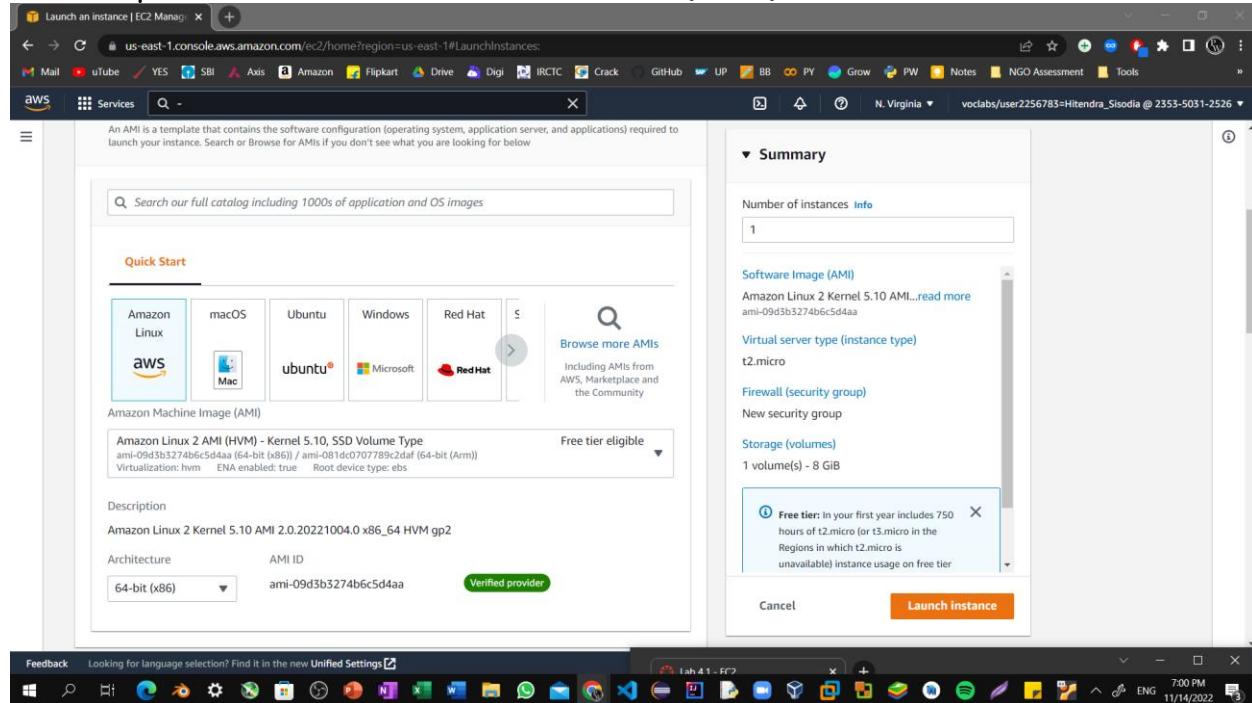
The screenshot shows the 'Launch an instance' wizard. In the 'Name and tags' step, the 'Name' field is filled with 'HitendraSisodia'. In the 'Summary' section on the right, it shows 'Number of instances' set to 1. Under 'Software Image (AMI)', it lists 'Amazon Linux 2 Kernel 5.10 AMI...' with AMI ID ami-0943b53274b6cc5d4aa. The 'Virtual server type (instance type)' is set to 't2.micro'. A tooltip for 'Free tier' indicates it includes 750 hours of t2.micro usage in N. Virginia. At the bottom right, there are 'Cancel' and 'Launch instance' buttons.

## Lab 11: Launching an EC2 Instance With EBS Storage

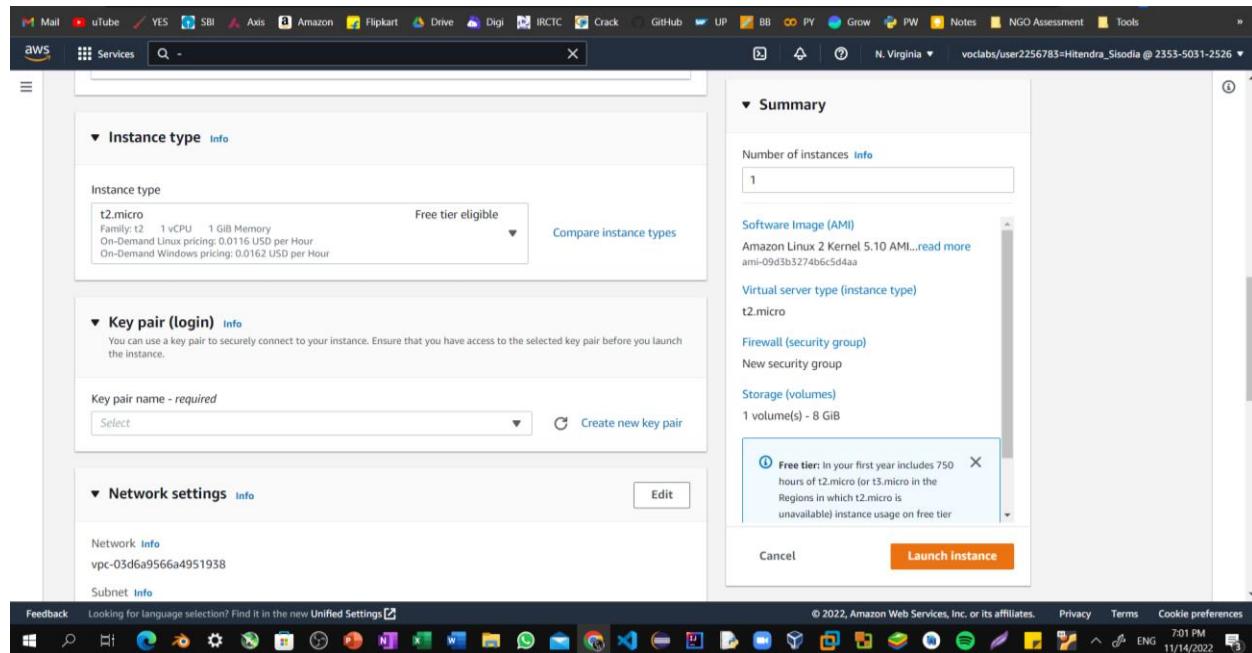
Step5: Choose an AMI from which to create the instance:

In the list of available Quick Start AMIs, keep the default Amazon Linux AMI selected.

Also keep the default Amazon Linux 2 AMI (HVM) selected.

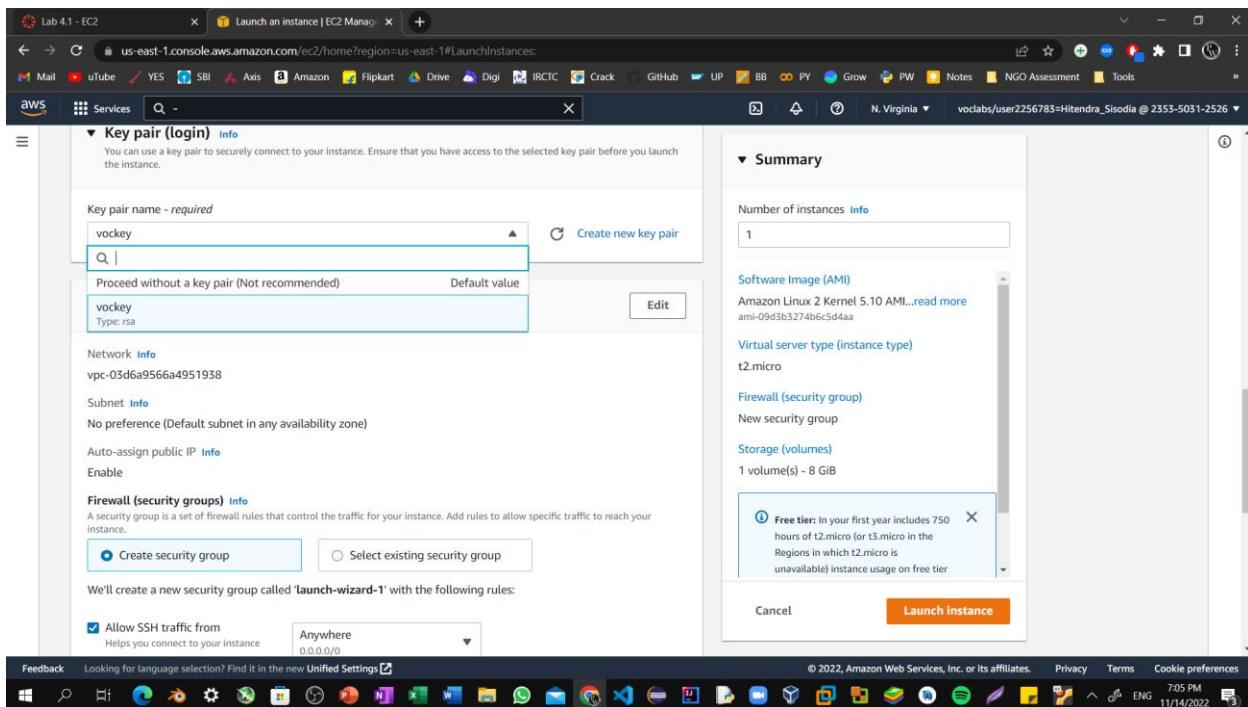


Step6: Specify an Instance type: In the Instance type panel, keep the default t2.micro selected.

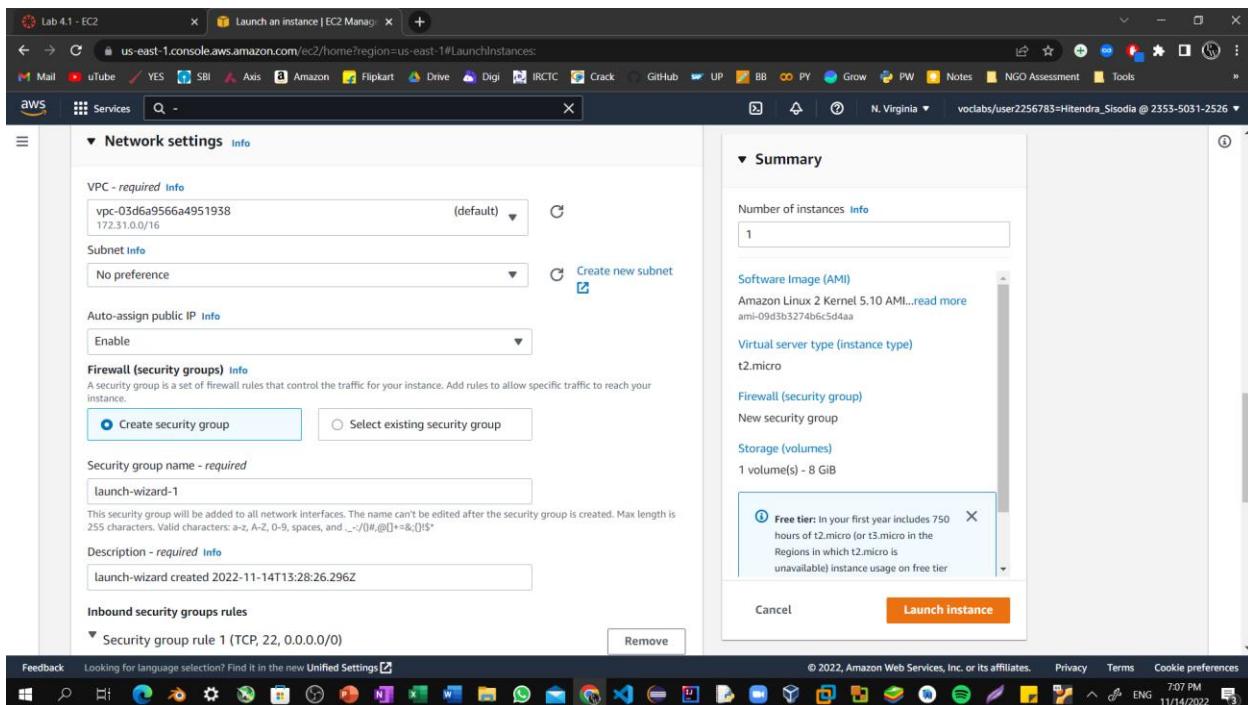


## Lab 11: Launching an EC2 Instance With EBS Storage

Step7: Select the key pair to associate with the instance. From the Key pair name menu, select **vockey**.

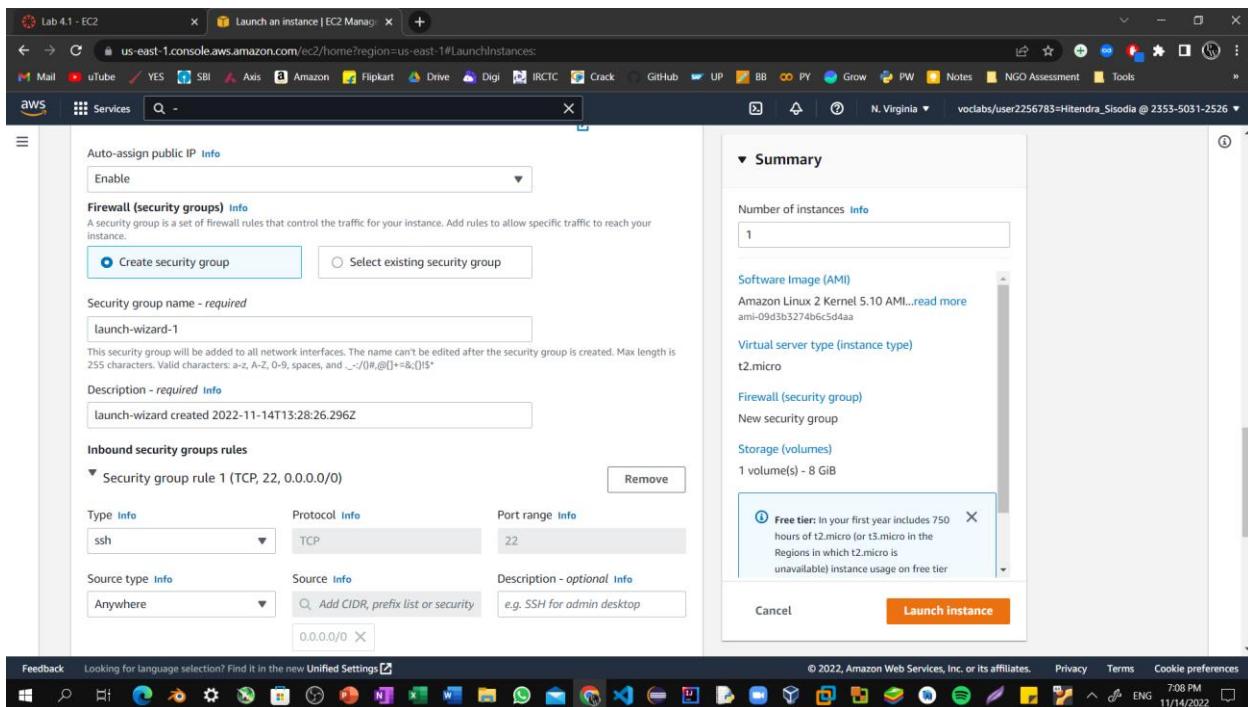


Step8: Next to Network settings, choose **Edit**. Keep the default VPC and subnet settings. Also keep the **Auto-assign public IP** setting set to **Enable**.



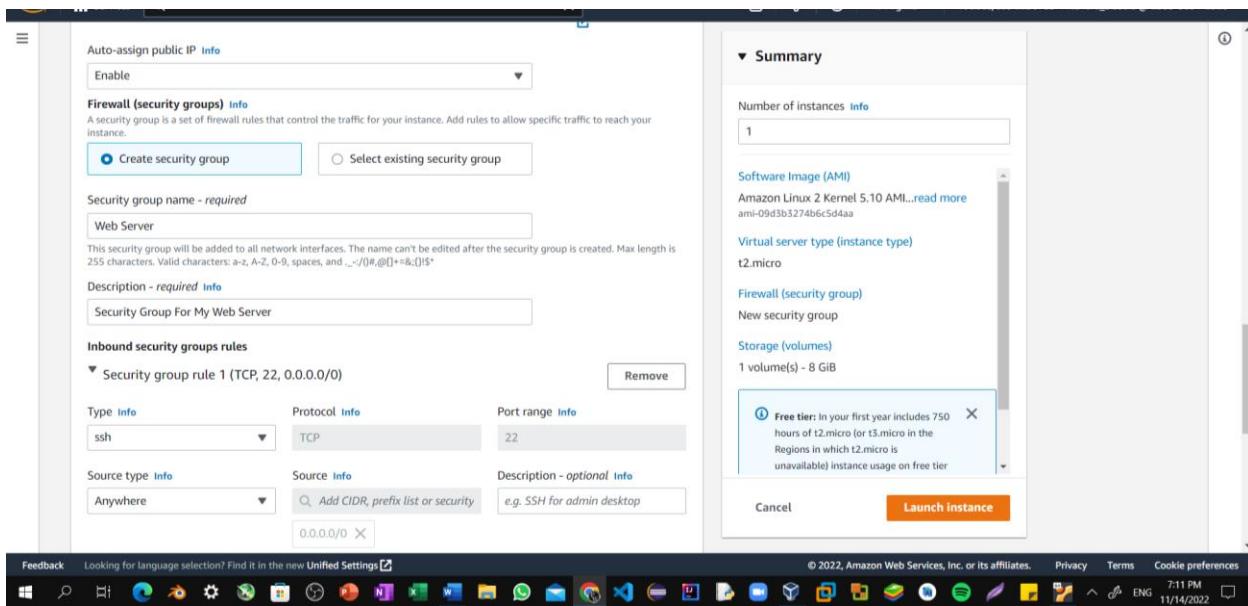
## Lab 11: Launching an EC2 Instance With EBS Storage

Step9: Under Firewall (security groups), keep the default **Create security group** option chosen.



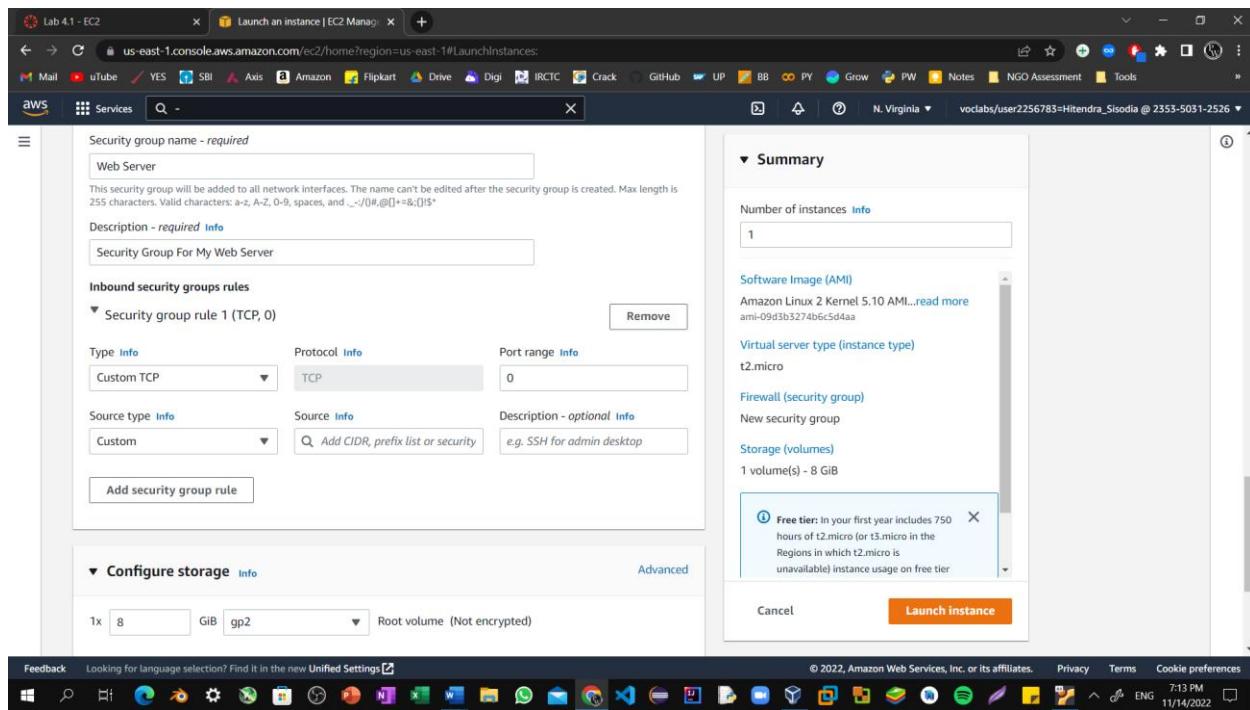
Step10: Configure a new security group:

- Keep the default selection **Create a new security group**.
- Security group name:** Clear the text and enter **Web Server**
- Description:** Clear the text and enter **Security group for my web server**

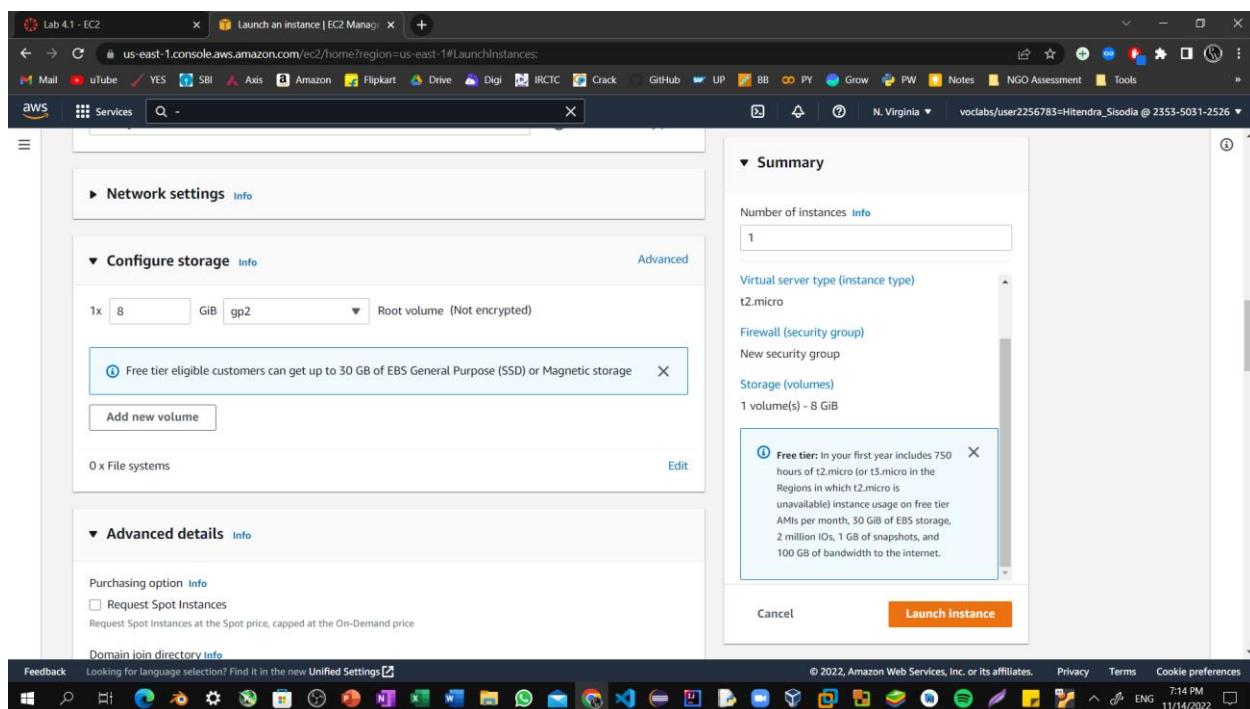


## Lab 11: Launching an EC2 Instance With EBS Storage

Step11: Choose Remove to remove the default SSH inbound rule.



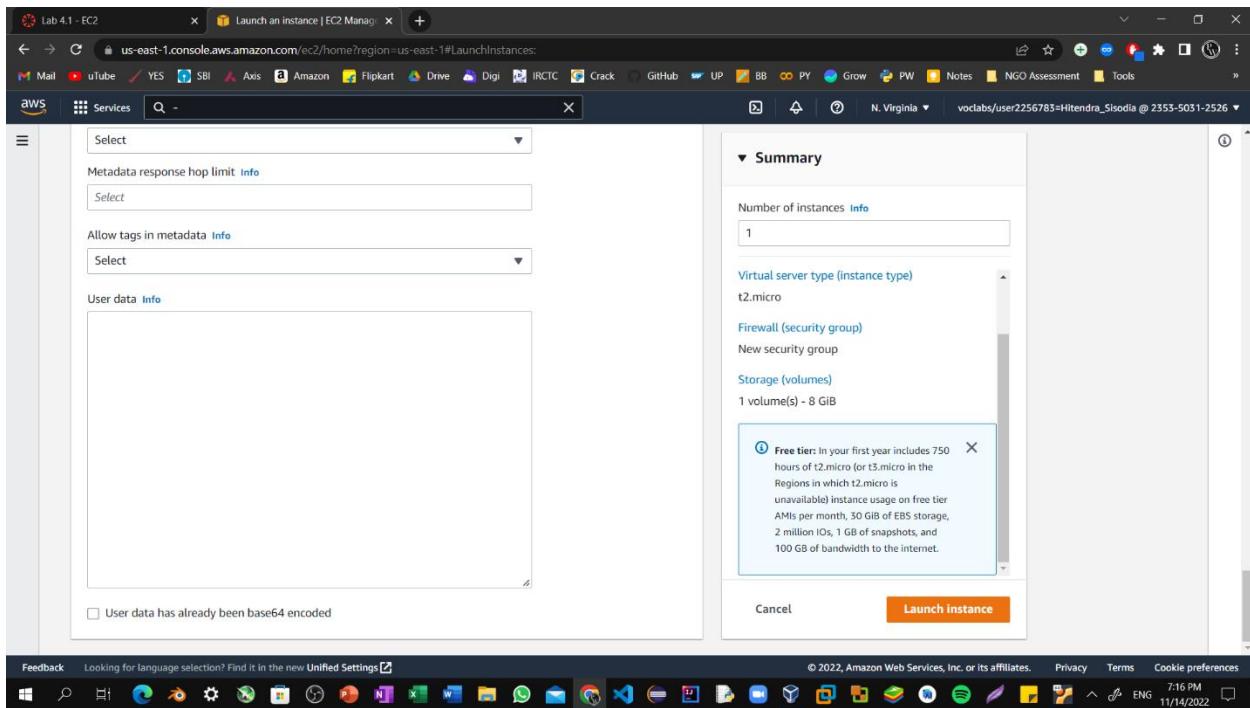
Step12: In the *Configure storage* section, keep the default settings. You will launch the Amazon EC2 instance using a default Elastic Block Store (EBS) disk volume.



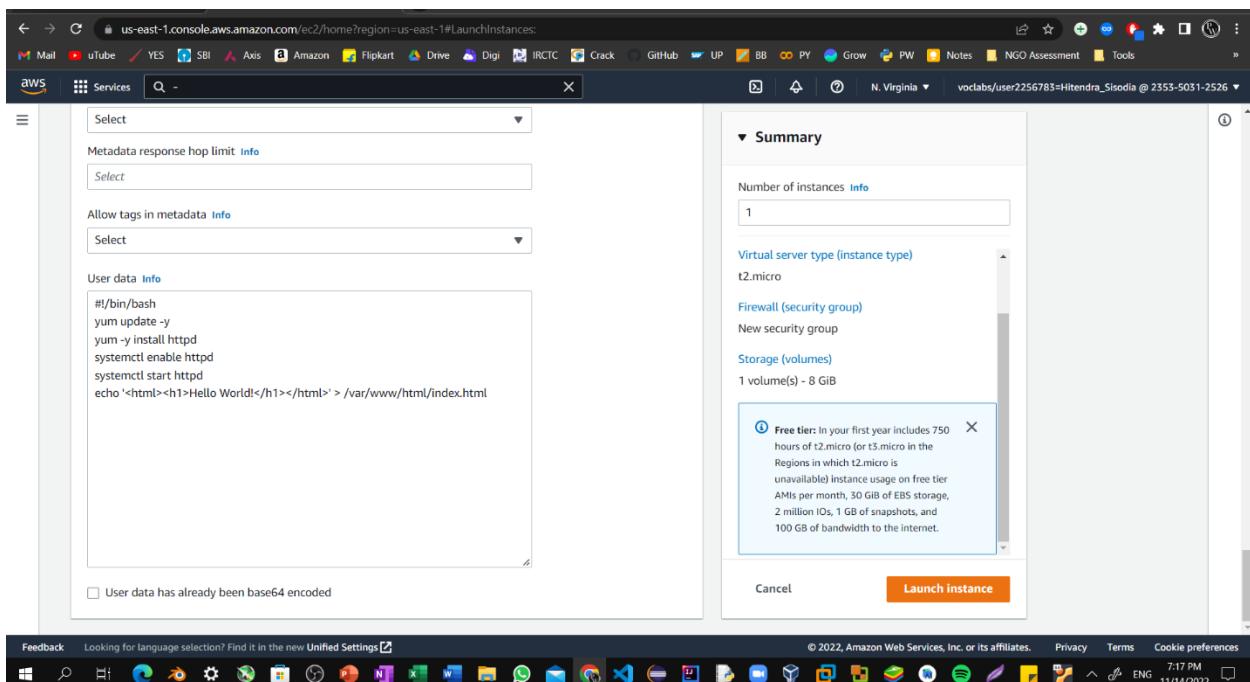
## Lab 11: Launching an EC2 Instance With EBS Storage

Step13: Configure a script to run on the instance when it launches:

- Expand the **Advanced details** panel.

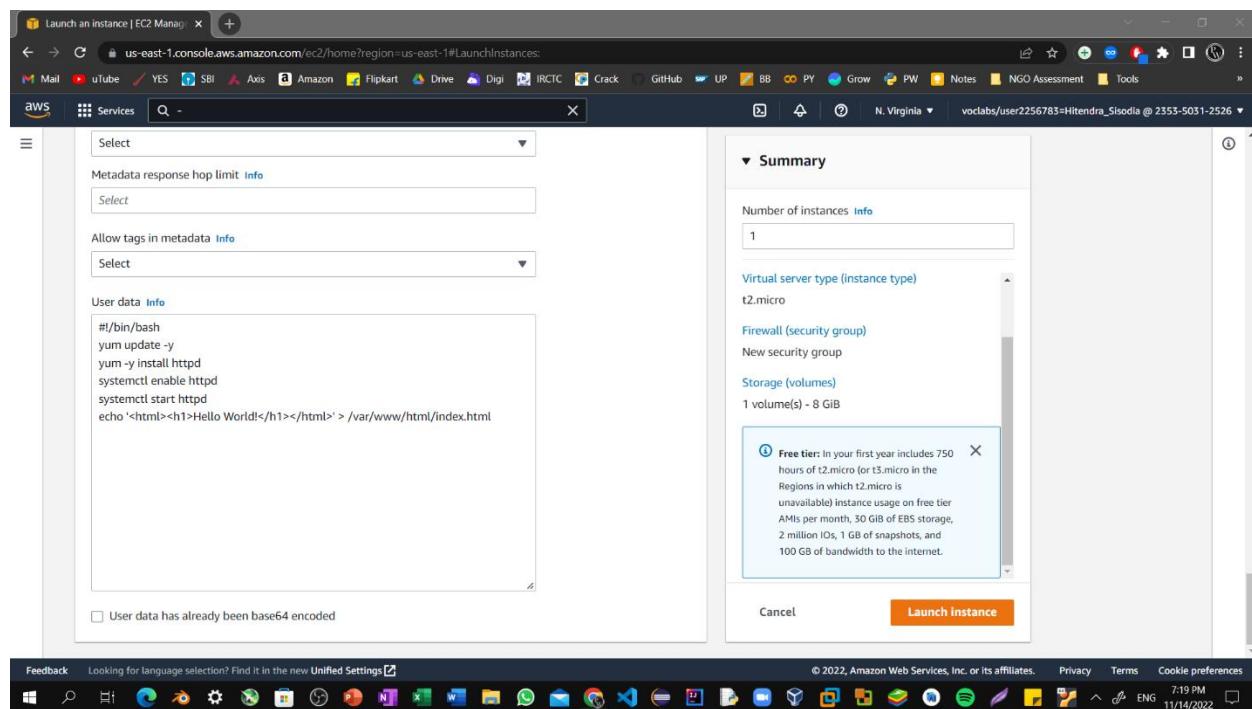


Step14: Scroll to the bottom of the page and then copy and paste the code shown below into the **User data** box.

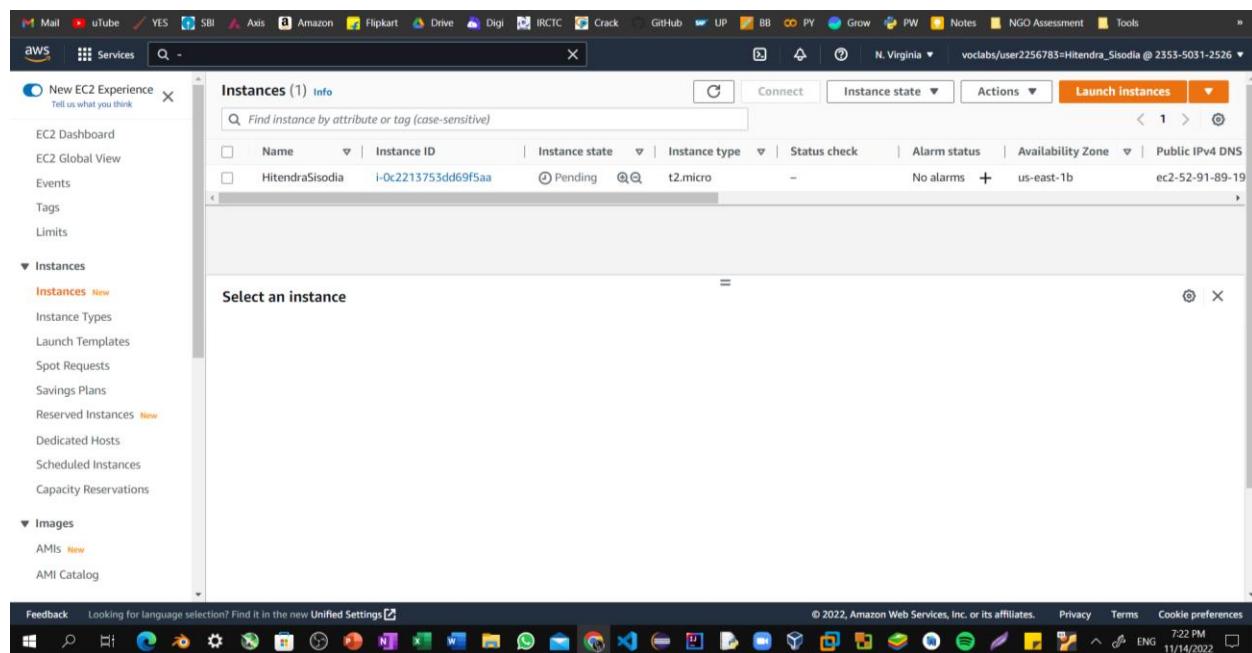


## Lab 11: Launching an EC2 Instance With EBS Storage

Step15: At the bottom of the **Summary** panel on the right side of the screen choose **Launch Instances**. You will see a Success message.



Step16: The instance will first appear in the *Pending* state, which means it is being launched. The state will then change to *Running*, which indicates that the instance has started booting. It takes a few minutes for the instance to boot.



## Lab 11: Launching an EC2 Instance With EBS Storage

Step17: Before you continue, wait for your instance to display the following:

**Instance state: Running**

**Status check: 2/2 checks passed**

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with options like EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (selected), and Images. The main area displays a table titled 'Instances (1) Info'. It shows one instance: 'HitendraSisodia' (Instance ID: i-0c2213753dd69f5aa), which is 'Running' (Status check: 2/2 checks passed). The table includes columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. At the bottom of the main area, a modal window titled 'Select an instance' is open, showing the same instance information.

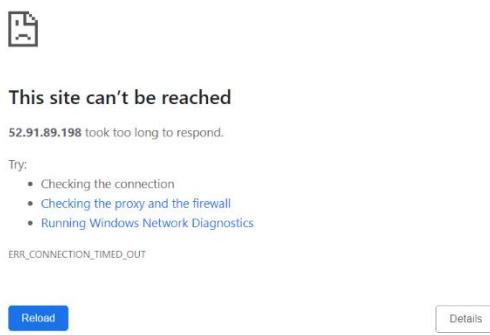
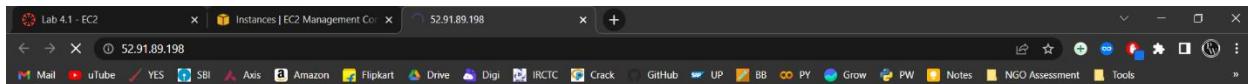
Step18: From the Details tab, copy the Public IPv4 address value of your instance to your clipboard.

The screenshot shows the AWS EC2 Instances page with the 'Details' tab selected for the instance 'i-0c2213753dd69f5aa'. In the 'Details' section, the 'Public IPv4 address' field is highlighted, showing the value '52.91.89.198'. Below this, the 'Instance summary' section provides more details about the instance, including its Instance ID, IP name, Hostname type, and Instance type. The status bar at the bottom indicates the instance is running.

## Lab 11: Launching an EC2 Instance With EBS Storage

**Step19:** Open a new tab in your web browser, paste the public IP address you just copied, and press **Enter**.

The webpage does not load. You must update the security group to be able to access the page.



**Step20:** Return to the **EC2 Management Console** browser tab.

In the left navigation pane, under **Network & Security**, choose **Security Groups**.

Name	Security group ID	Security group name	VPC ID	Description	Owner
-	sg-0628e6ae9e7e6ad67	Web Server	vpc-03d6a9566a4951938	Security Group For My ...	235350312526
-	sg-00aaeceedad87b2b1	default	vpc-03d6a9566a4951938	default VPC security gr...	235350312526

## Lab 11: Launching an EC2 Instance With EBS Storage

Step21: Select the **Web Server** security group, which you created when launching your EC2 instance. In the lower pane, choose the **Inbound rules** tab.

The screenshot shows the AWS EC2 Management Console. On the left, there's a navigation sidebar with options like AMIs, Elastic Block Store, Network & Security, Load Balancing, Auto Scaling, and Services. Under Services, 'Security Groups' is selected. The main pane displays a table of security groups. One row is selected, showing details: Name: Web Server, Security group ID: sg-0628e6ae9e7e6ad67, Security group name: Web Server, VPC ID: vpc-03d6a9566a4951958, Description: Security Group For My ..., Owner: 235350312526. Below the table, tabs for 'Details', 'Inbound rules', 'Outbound rules', and 'Tags' are visible, with 'Inbound rules' being the active tab. A note says 'You can now check network connectivity with Reachability Analyzer' with a 'Run Reachability Analyzer' button. At the bottom, a message says 'No security group rules found'.

Step22: Choose **Edit inbound rules**, and then choose **Add rule**.

The screenshot shows the 'Edit inbound rules' page for the 'sg-0628e6ae9e7e6ad67 - Web Server' security group. The top navigation bar shows the path: EC2 > Security Groups > sg-0628e6ae9e7e6ad67 - Web Server > Edit inbound rules. The main area is titled 'Inbound rules' with a 'Info' link. It has columns for Security group rule ID, Type, Protocol, Port range, Source, and Description - optional. A single rule is listed: Type: Custom TCP, Protocol: TCP, Port range: 0, Source: Custom. Below the table is a 'Delete' button. At the bottom, there are 'Cancel', 'Preview changes', and 'Save rules' buttons. The status bar at the bottom indicates English (US), 7:34 PM, and 11/14/2022.

## Lab 11: Launching an EC2 Instance With EBS Storage

Step23: Configure the following:

Type: HTTP

Source: Anywhere-IPv4 Choose Save rules

The screenshot shows the AWS EC2 Management Console with the URL [us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#SecurityGroups](https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#SecurityGroups). A success message at the top states: "Inbound security group rules successfully modified on security group (sg-0628e6ae9e7e6ad67 | Web Server) Details". The main table lists two security groups:

Name	Security group ID	VPC ID	Description	Owner
-	sg-00aeceead87b2b1	vpc-03d6a9566a4951938	default VPC security gr...	235350312526
<input checked="" type="checkbox"/>	sg-0628e6ae9e7e6ad67	vpc-03d6a9566a4951938	Web Server Security Group For My ...	235350312526

Below the table, a message says: "You can now check network connectivity with Reachability Analyzer". A "Run Reachability Analyzer" button is available. The status bar at the bottom right shows: "© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms 7:37 PM ENG 11/14/2022".

Step24: Return to the tab that you used to try to connect to the web server. The page should display the message *Hitendra Sisodia*.

The screenshot shows a web browser window with the URL [52.91.89.198](http://52.91.89.198). The page content displays the text "Hitendra Sisodia". The browser's address bar shows "Not secure | 52.91.89.198". The status bar at the bottom right shows: "7:38 PM ENG 11/14/2022".

## Lab 11: Launching an EC2 Instance With EBS Storage

Step25: Return to the **EC2 Management Console** browser tab.

The screenshot shows the AWS EC2 Management Console interface. In the left navigation pane, under 'Instances', the 'Instances' link is selected. The main content area displays a table titled 'Instances (1) Info' with one row. The row contains the instance name 'HitendraSisodi...', instance ID 'i-06e85687ed5bf30bf', state 'Running', type 't2.micro', and availability zone 'us-east-1a'. A status bar at the bottom right indicates 'ec2-44-210-129-10'. The taskbar at the bottom shows various application icons.

Step26: In the left navigation pane, under **Instances**, choose **Instances**. Select the **Web Server** instance, and in the **Networking** tab below, note the **Availability Zone** in which your instance is running.

The screenshot shows the AWS EC2 Management Console interface with the 'Instances' link selected in the left navigation pane. The main content area displays the same instance details as the previous screenshot. Below the instance table, there is a section titled 'Instance: i-06e85687ed5bf30bf (HitendraSisodiaEC2)'. Under this section, the 'Availability zone' field is set to 'us-east-1a'. The taskbar at the bottom shows various application icons.

## Lab 11: Launching an EC2 Instance With EBS Storage

Step27: In the left navigation pane, under **Elastic Block Store**, select **Volumes**.

You can now create Amazon Data Lifecycle Manager policies to automate snapshot management directly from this screen. Select the volumes to back up, and then choose **Actions**, **Create snapshot lifecycle policy**. For more information, see the Knowledge Center article.

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Avail
-	vol-090ad190ed6091397	gp2	8 GiB	100	-	snap-0c0b30d...	2022/11/14 21:29 GMT+5:...	us-e...

Select a volume above

Step28: Select **Create volume**.

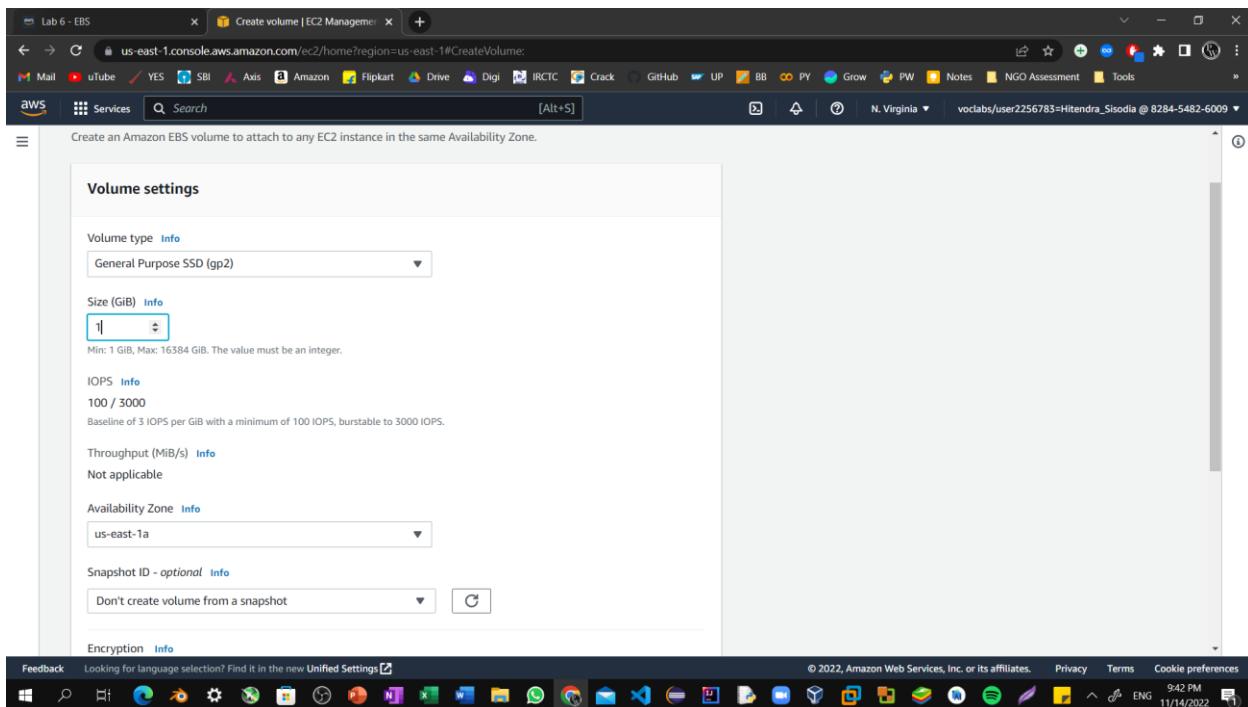
You can now create Amazon Data Lifecycle Manager policies to automate snapshot management directly from this screen. Select the volumes to back up, and then choose **Actions**, **Create snapshot lifecycle policy**. For more information, see the Knowledge Center article.

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot	Created	Avail
-	vol-090ad190ed6091397	gp2	8 GiB	100	-	snap-0c0b30d...	2022/11/14 21:29 GMT+5:...	us-e...

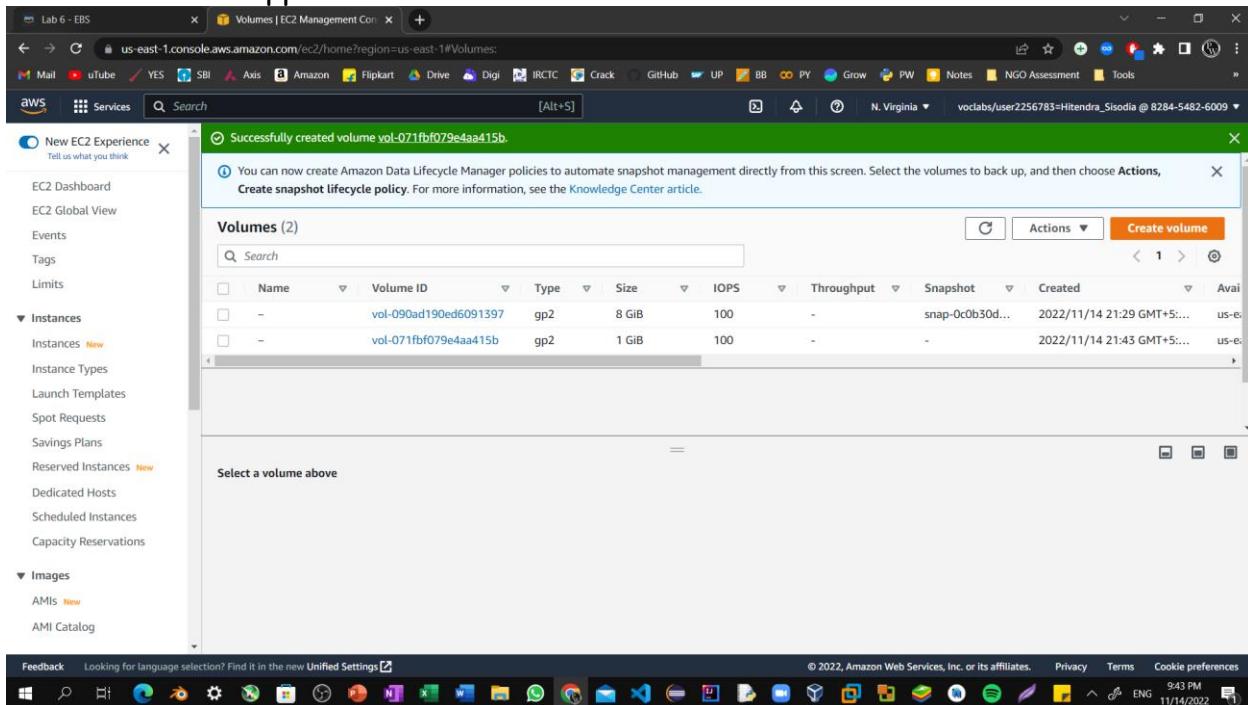
Select a volume above

## Lab 11: Launching an EC2 Instance With EBS Storage

**Step29:** For **Size**, enter **1** to create a volume with 1 GiB. For **Availability Zone**, select the same Availability Zone that your EC2 instance is running in.



**Step30:** Scroll down and select **Create volume**.  
The new volume appears in the volumes list with a state of **available**.



## Lab 11: Launching an EC2 Instance With EBS Storage

Step31: Select the new 1 GiB size volume. Then, choose Actions, and Select Attach volume.

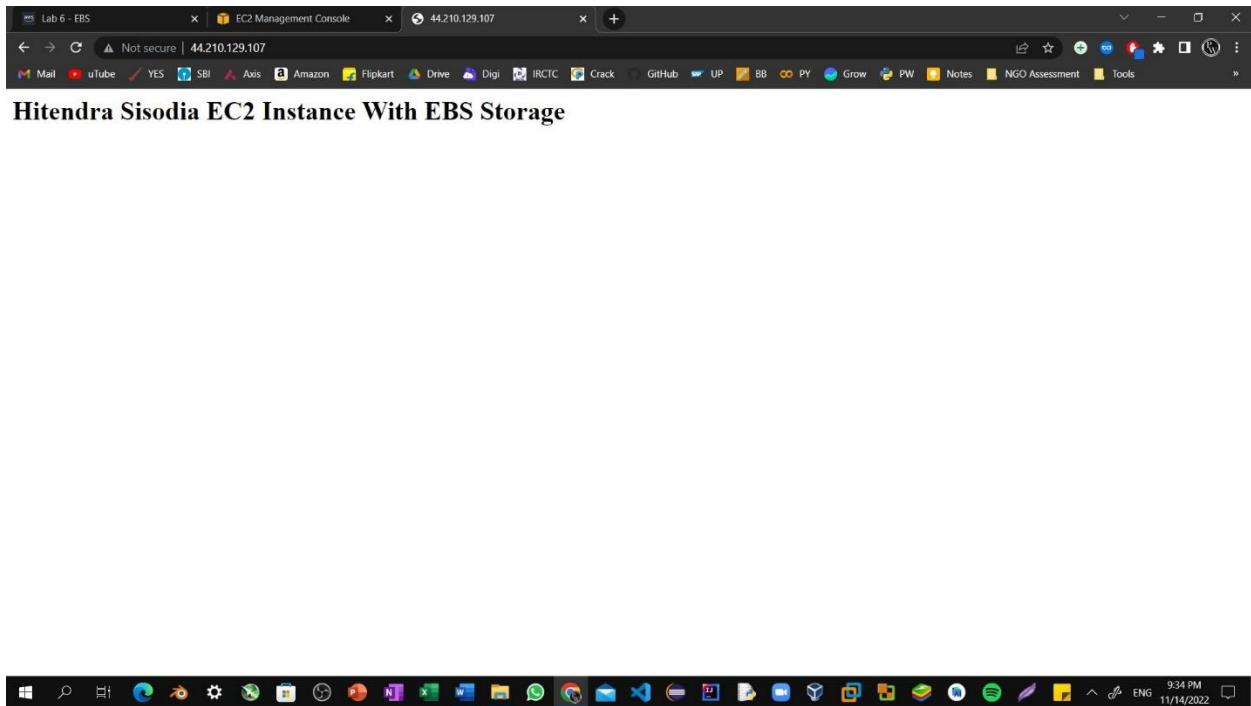
The screenshot shows the AWS EBS Volumes Management console. On the left, there's a sidebar with navigation links for EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations), and Images (AMIs, AMI Catalog). The main area displays a table of volumes. One volume, 'vol-071fbf079e4aa415b' (Size: 1 GiB, Type: gp2), is selected and highlighted with a checkmark. An info message at the top right says: 'You can now create Amazon Data Lifecycle Manager policies to automate snapshot management directly from this screen. Select the volumes to back up, and then choose Actions, Create snapshot lifecycle policy. For more information, see the Knowledge Center article.' Below the table, a detailed view for the selected volume is shown, including its Volume ID, Size (1 GiB), Type (gp2), Volume state (IOPS), Throughput, Volume status (Okay), and Encryption status. The Actions button in the top right dropdown menu is highlighted, and the 'Attach volume' option is visible in the list.

Step32: Select the **Instance** drop-down menu, and then select your EC2 instance. The list of instances will automatically populate.

The screenshot shows the 'Attach volume' dialog box. At the top, it says 'Attach a volume to an instance to use it as you would a regular physical hard disk drive.' Below this is a 'Basic details' section with fields for 'Volume ID' (set to 'vol-071fbf079e4aa415b') and 'Availability Zone' (set to 'us-east-1'). Under 'Instance Info', a dropdown menu shows the selected EC2 instance: 'i-06e85687ed5bf30bf'. A note below the dropdown states: 'Only instances in the same Availability Zone as the selected volume are displayed.' In the bottom right corner of the dialog, there are 'Cancel' and 'Attach volume' buttons. The status bar at the bottom of the browser window shows the date and time as '11/14/2022 9:44 PM'.

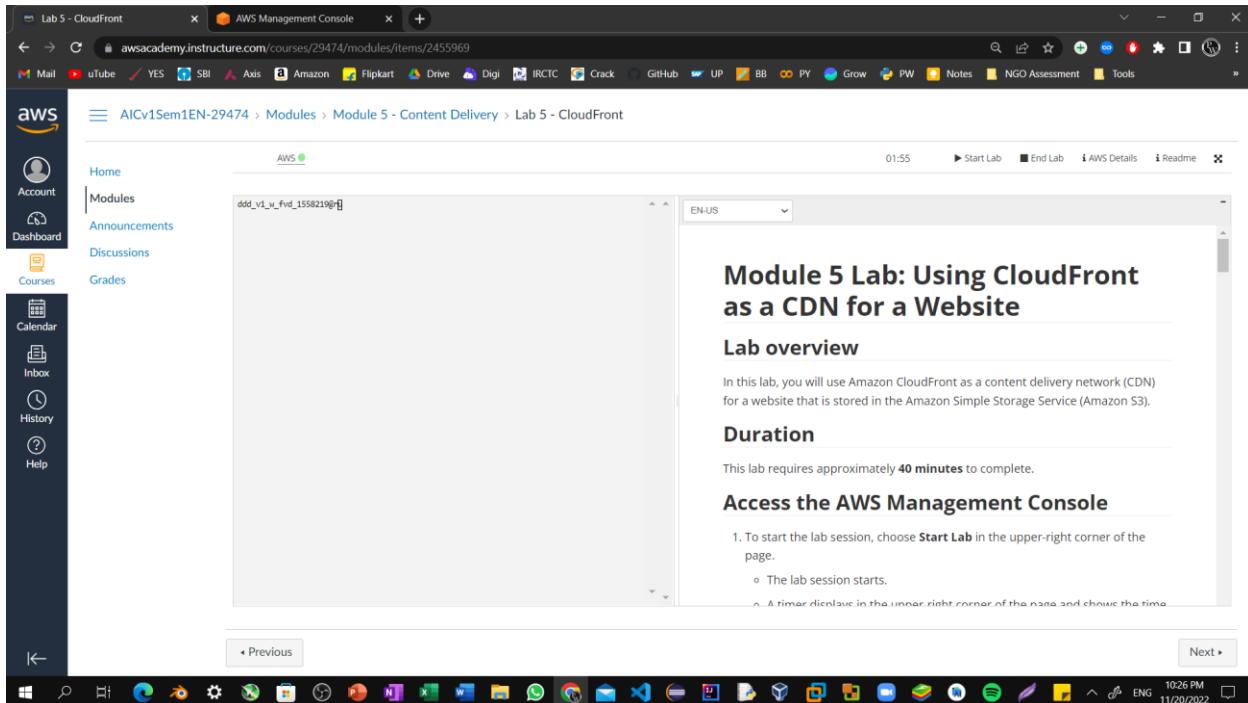
### Step33: Select Attach volume.

The state of the volume changes to *in-use*. The new volume is now attached to your EC2 instance. Refresh The webpage that we created using EC2 instance now updated with EBS Storage.

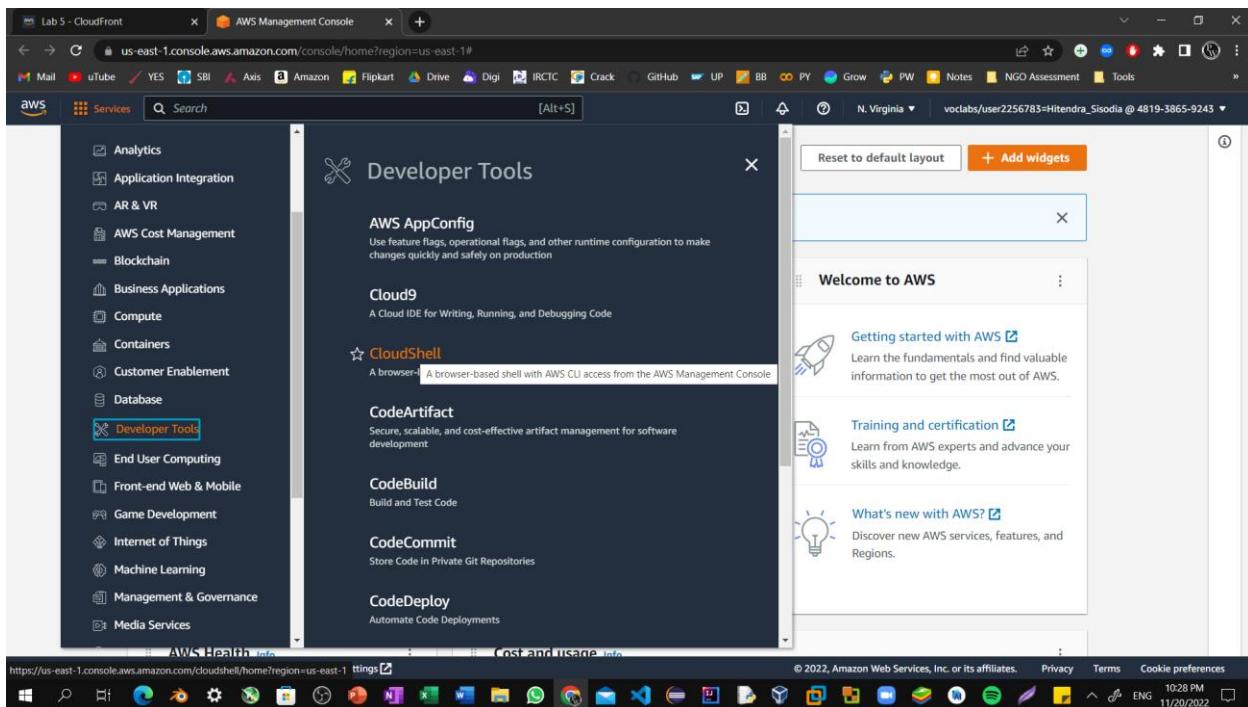


## Lab 12: Using CloudFront As a CDN For A Website

Step1: To start the lab session, choose **Start Lab** in the upper-right corner of the page.

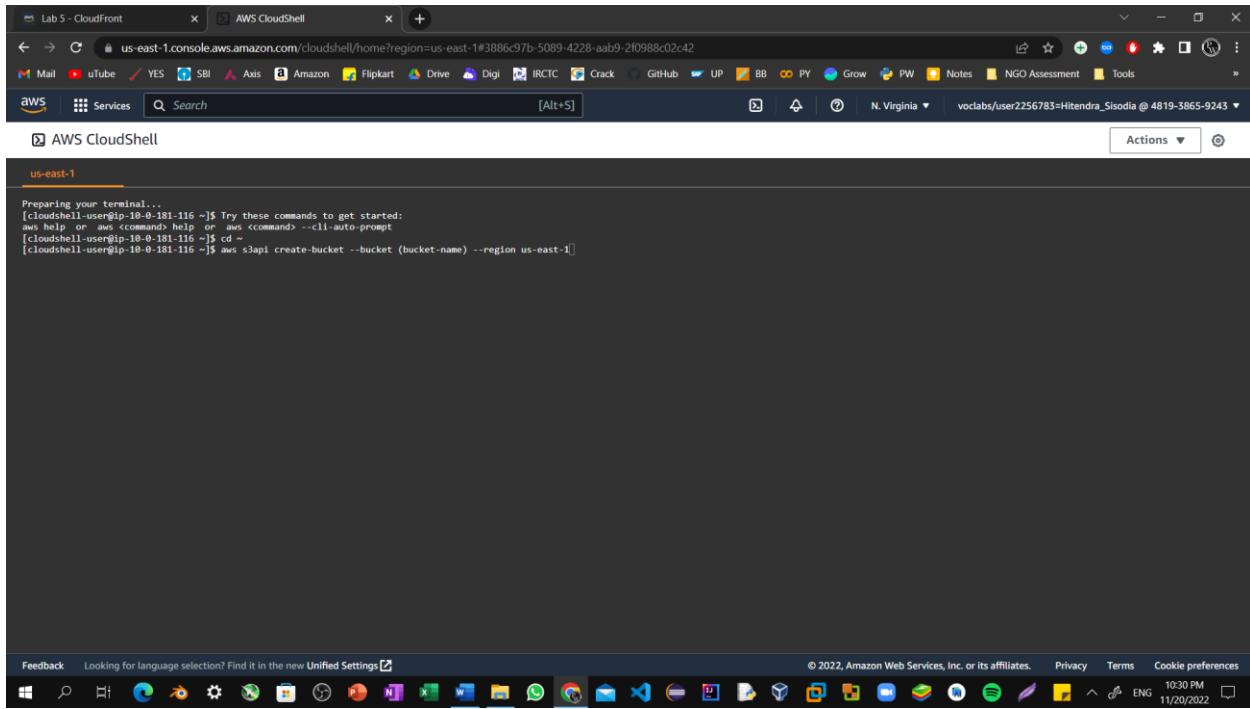


Step2: Choose the **Services** menu, locate the **Developer Tools** services, and select **CloudShell**. If a welcome pop-up window appears, choose **Close**.



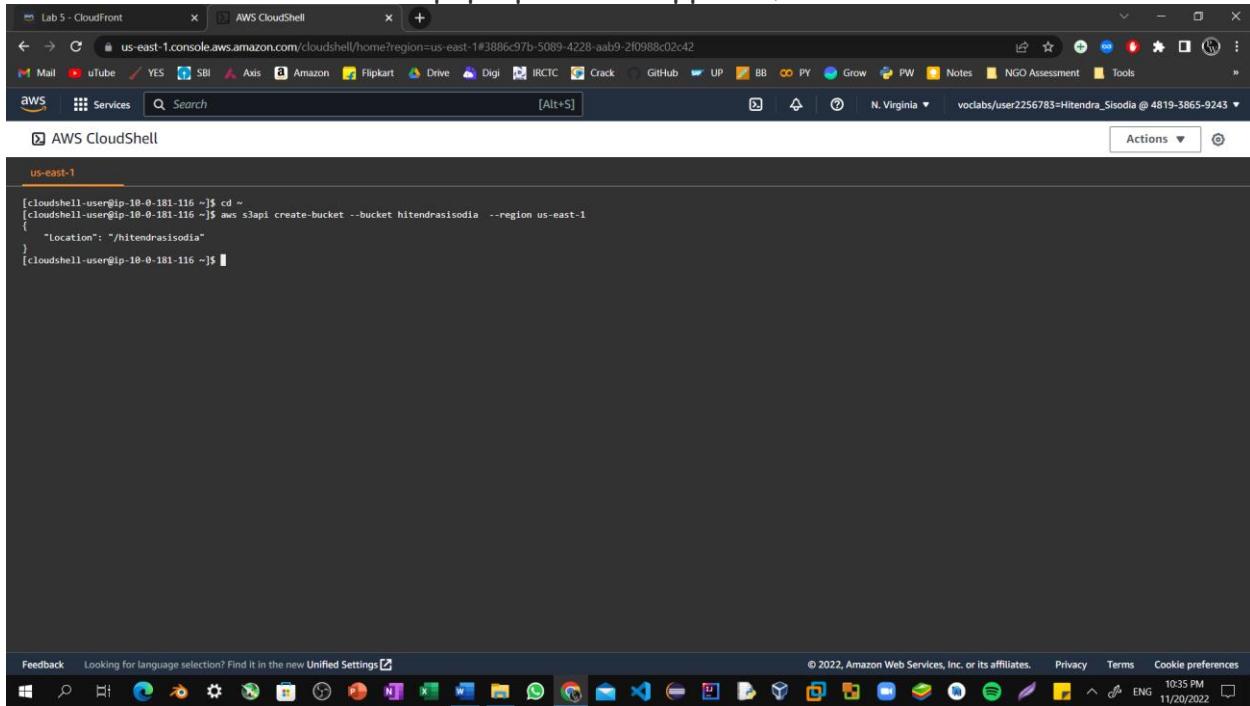
## Lab 12: Using CloudFront As a CDN For A Website

Step3: Copy and paste the following code into a text editor



The screenshot shows a Windows desktop environment with a browser window titled "Lab 5 - CloudFront" open to the AWS CloudShell interface. The terminal window is titled "us-east-1". The user has run the command "aws s3api create-bucket --bucket (bucket-name) --region us-east-1" and is awaiting further input. The AWS toolbar at the top includes links for Mail, YouTube, YES, SBI, Axis, Amazon, Flipkart, Drive, Digi, IRCTC, Crack, GitHub, UP, BB, PY, Grow, PW, Notes, NGO Assessment, and Tools. The status bar at the bottom right shows "ENG 11/20/2022" and "10:30 PM".

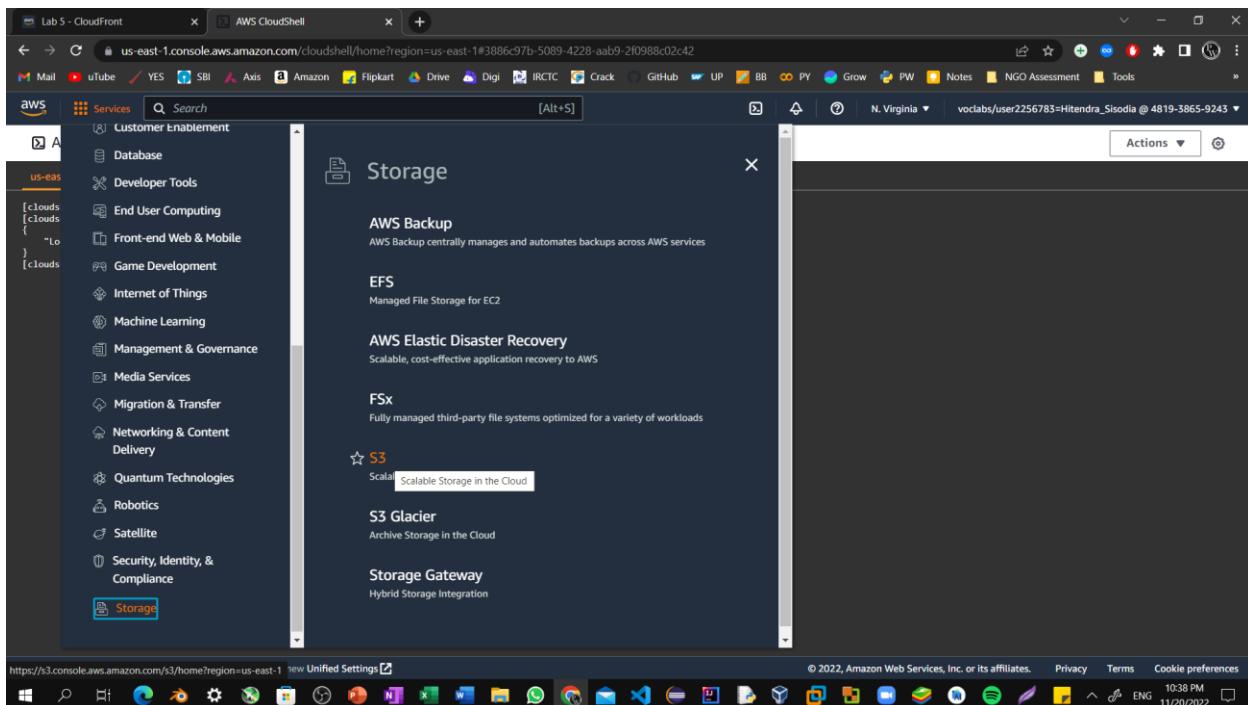
Step4: In the code that you copied, replace **(bucket-name)** with a unique Domain Name System (DNS)-compliant name for your new bucket. Run the updated code in the CloudShell terminal. If a pop-up window appears, choose Paste.



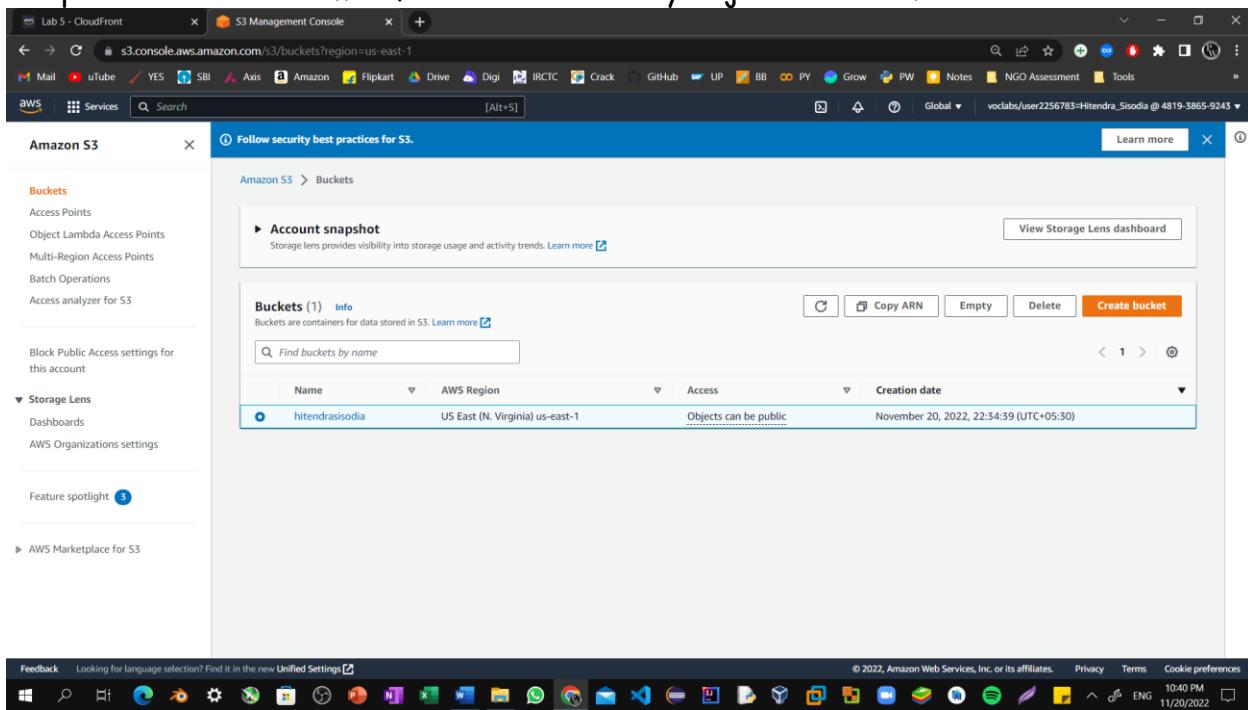
The screenshot shows the same AWS CloudShell interface as the previous one, but the user has replaced "(bucket-name)" with "hitendrasisodia". The terminal now displays the output of the command, including the bucket's location: "/hitendrasisodia". The AWS toolbar and status bar remain the same.

## Lab 12: Using CloudFront As a CDN For A Website

Step5: In the console, choose the **Services** menu, locate the **Storage** section, and choose **S3**.



Step6: Choose the name of the bucket that you just created.



## Lab 12: Using CloudFront As a CDN For A Website

### Step7: Choose the Permissions tab.

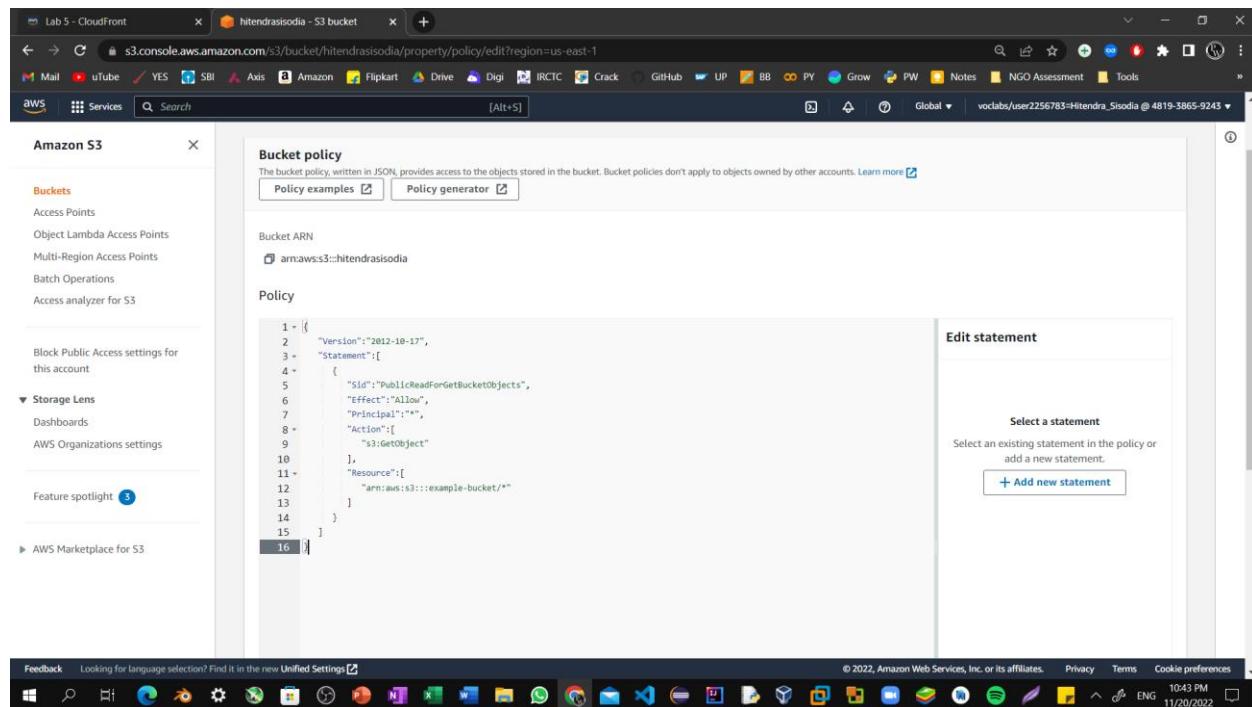
The screenshot shows the AWS S3 console with the 'Permissions' tab selected for the 'hitendrasisodia' bucket. Under the 'Block public access (bucket settings)' section, it is currently set to 'Off'. There is a link to 'Edit' these settings. The browser taskbar at the bottom shows various open tabs and system icons.

### Step8: In the Bucket policy section, choose Edit.

The screenshot shows the AWS S3 console with the 'Bucket policy' section selected. It displays a message stating 'No policy to display.' There is an 'Edit' button available for creating or modifying a policy. The browser taskbar at the bottom shows various open tabs and system icons.

## Lab 12: Using CloudFront As a CDN For A Website

Step9: To grant public read access for your website, copy and paste the following bucket policy into the policy editor.

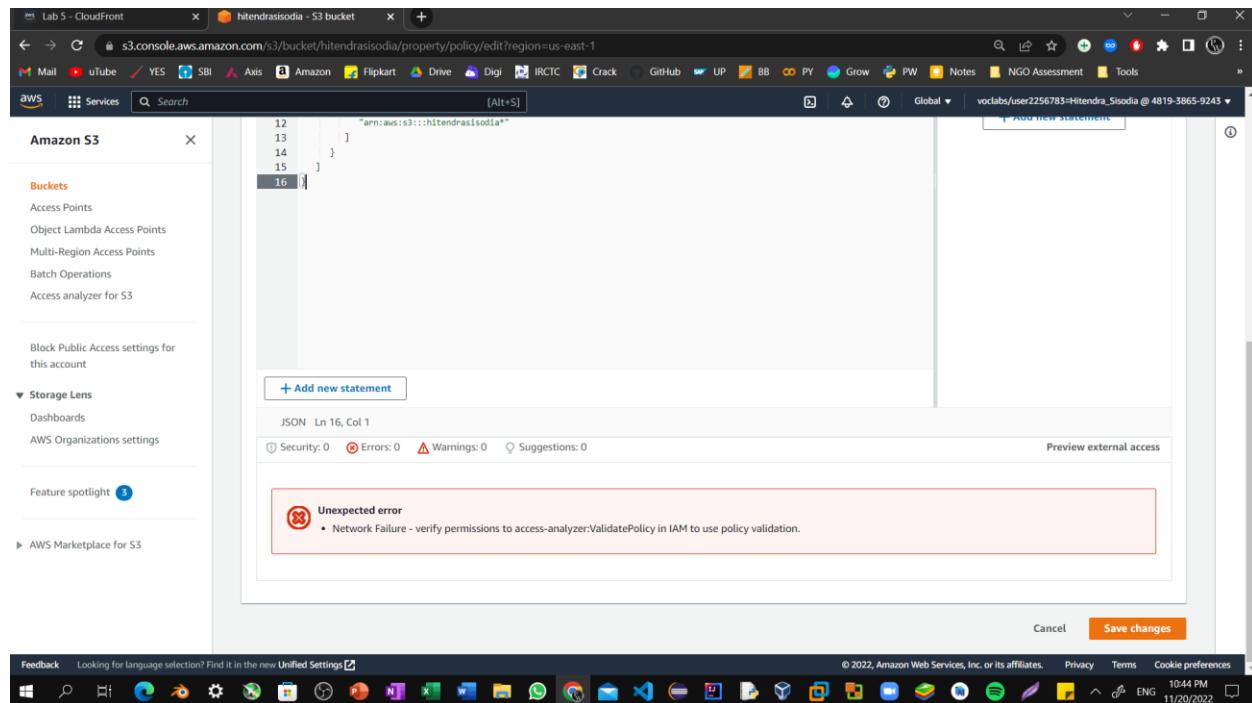


The screenshot shows the AWS S3 Bucket Policy editor. On the left, there's a sidebar with navigation links like Buckets, Storage Lens, and Feature spotlight. The main area is titled "Bucket policy" and contains a JSON code editor. The JSON code grants public read access to all objects in the bucket:

```
1 - {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "PublicReadForGetBucketObjects",
6       "Effect": "Allow",
7       "Principal": "*",
8       "Action": [
9         "s3:GetObject"
10      ],
11      "Resource": [
12        "arn:aws:s3:::example-bucket/*"
13      ]
14    }
15  ]
16 }
```

To the right of the code editor is a panel titled "Edit statement" with a sub-section "Select a statement" containing a button "+ Add new statement". At the bottom of the page, there's a "Save changes" button.

Step10: In the policy, replace **example-bucket** with the name of your bucket. At the bottom of the page, choose **Save changes**.



The screenshot shows the AWS S3 Bucket Policy editor after the bucket name has been replaced. The JSON code now reads:

```
12   "Resource": [
13     "arn:aws:s3:::hitendrasisodia/*"
14   ]
15 ]
16 }
```

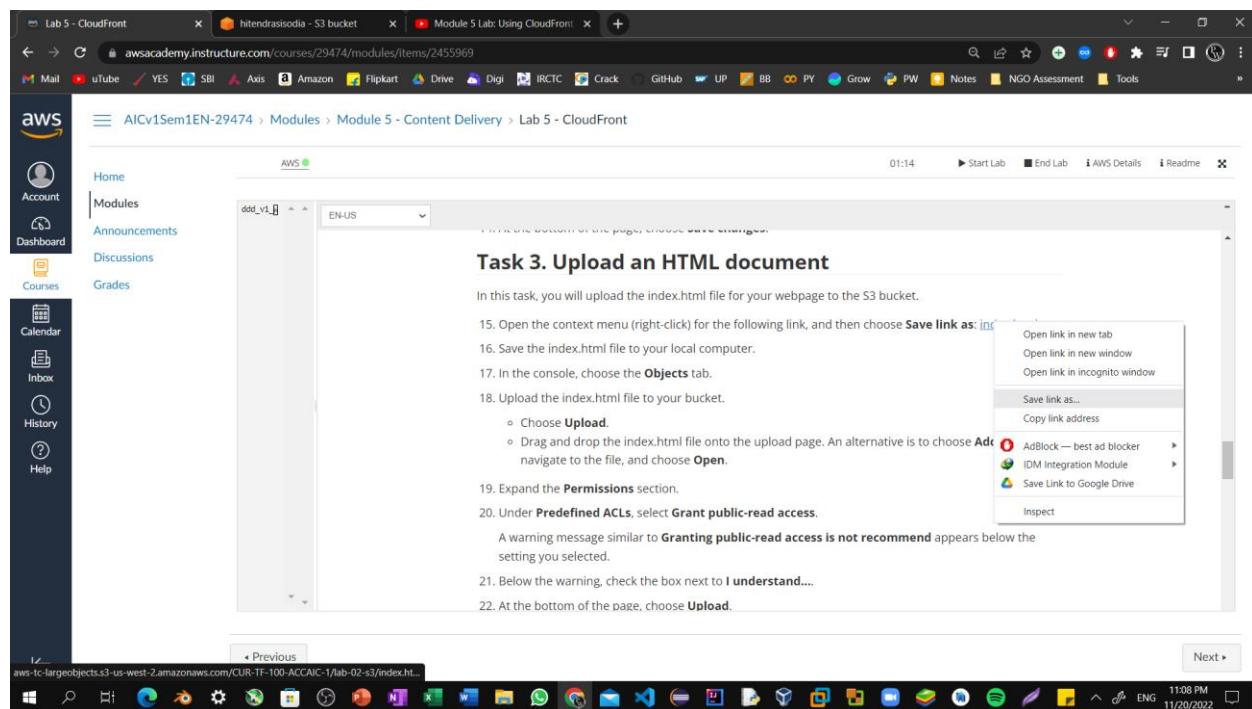
Below the code editor, there's an "Unexpected error" message box with the following details:

- Network Failure - verify permissions to access-analyzer:ValidatePolicy in IAM to use policy validation.

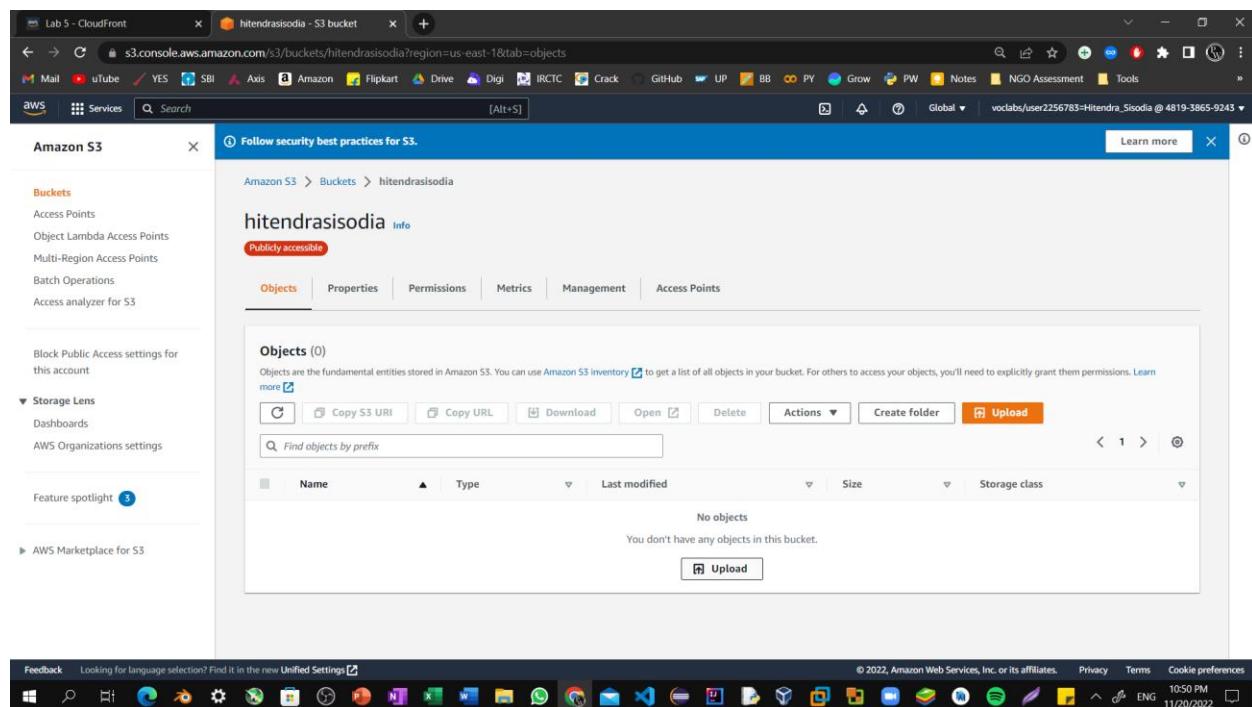
At the bottom right of the editor, there are "Cancel" and "Save changes" buttons. The status bar at the bottom of the browser window shows the time as 10:44 PM and the date as 11/20/2022.

## Lab 12: Using CloudFront As a CDN For A Website

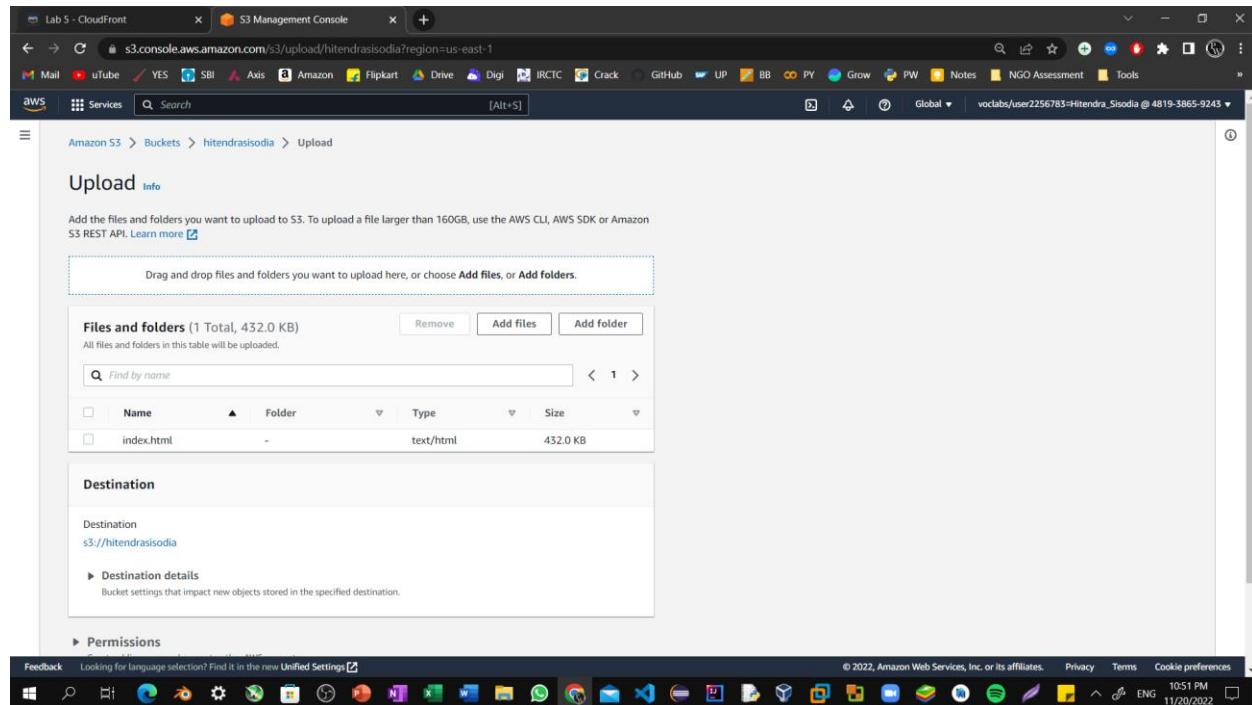
**Step10:** Open the context menu (right-click) for the following link, and then choose **Save link as:** index.html. Save the index.html file to your local computer.



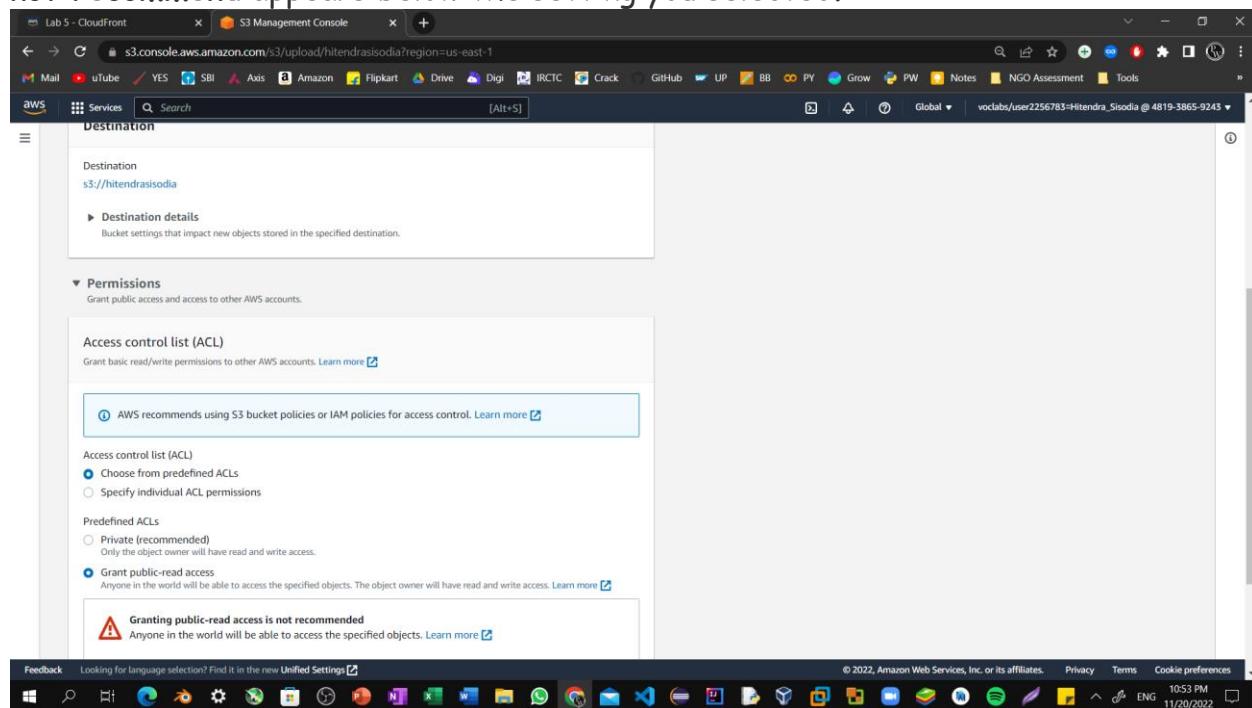
**Step11:** In the console, choose the **Objects** tab. Upload the index.html file to your bucket. Choose **Upload**. Drag and drop the index.html file onto the upload page.



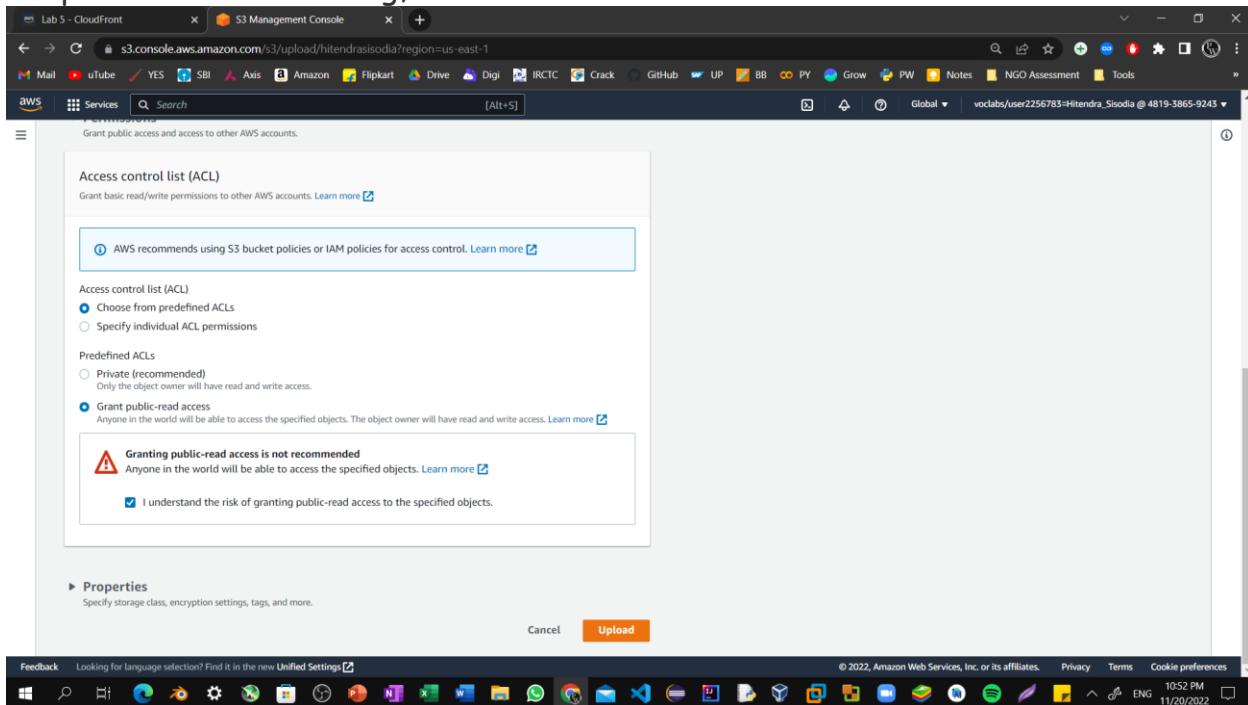
Step12: An alternative is to choose **Add files**, navigate to the file, and choose **Open**.



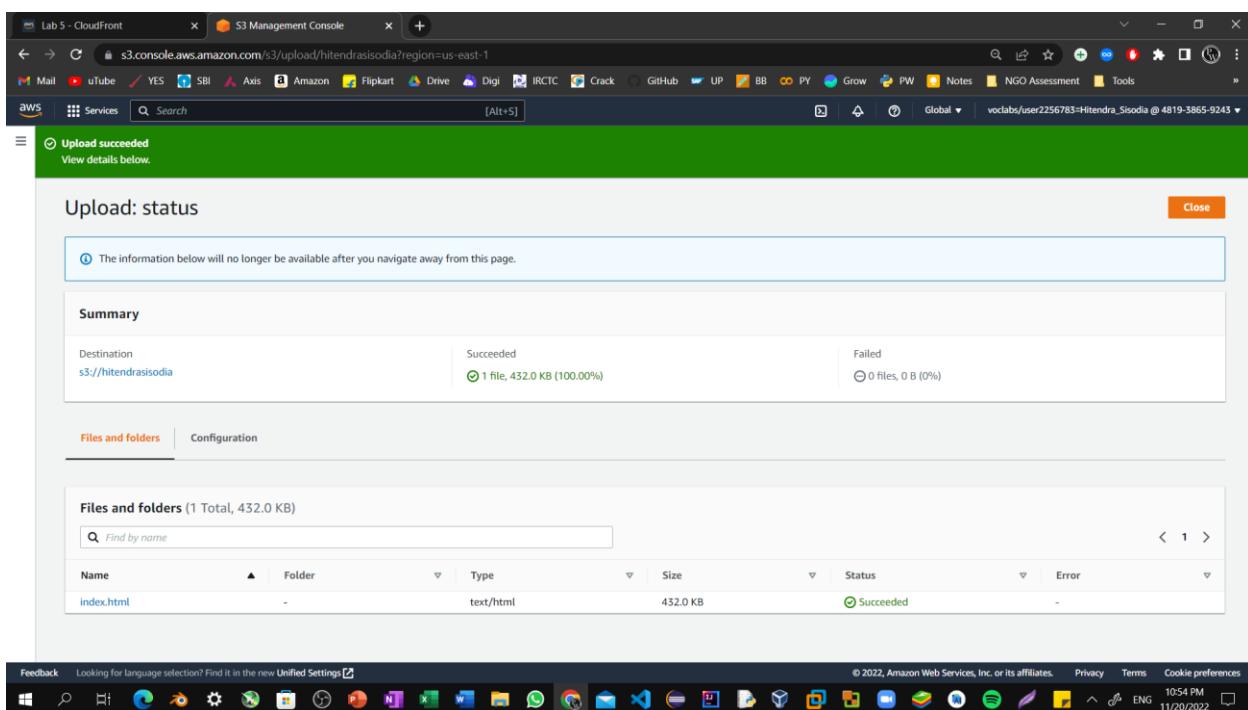
Step13: Expand the **Permissions** section. Under **Predefined ACLs**, select **Grant public-read access**. A warning message similar to **Granting public-read access is not recommended** appears below the setting you selected.



Step14: Below the warning, check the box next to I understand..



Step15: At the bottom of the page, choose Upload. Choose Close.



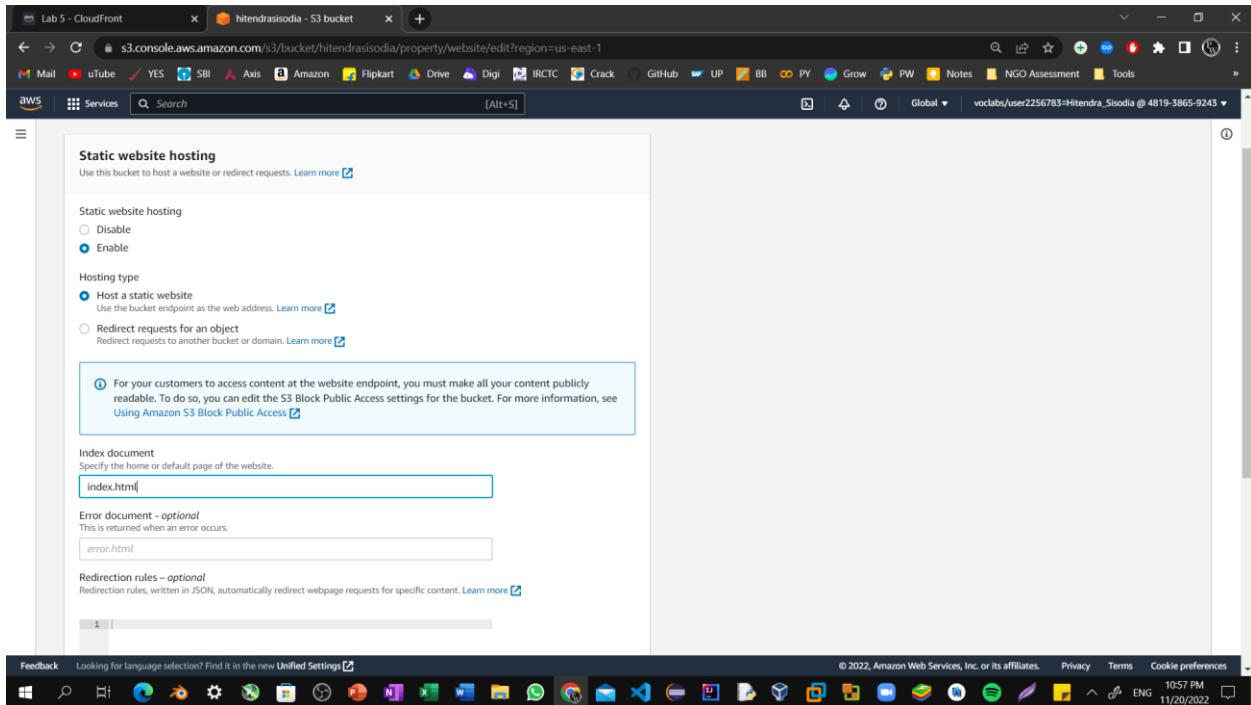
**Step16:** The index.html file appears in the Objects list.

The screenshot shows a browser window with the URL [s3.console.aws.amazon.com/s3/buckets/hitendrasisodia?region=us-east-1&tab=objects](https://s3.console.aws.amazon.com/s3/buckets/hitendrasisodia?region=us-east-1&tab=objects). The page displays the 'Objects' section of the 'hitendrasisodia' bucket. There is one object listed: 'index.html' (Type: html, Last modified: November 20, 2022, 22:54:42 (UTC+05:30), Size: 432.0 KB, Storage class: Standard). The 'Actions' menu is visible above the object list, with 'Upload' highlighted. The browser's taskbar at the bottom shows various pinned icons.

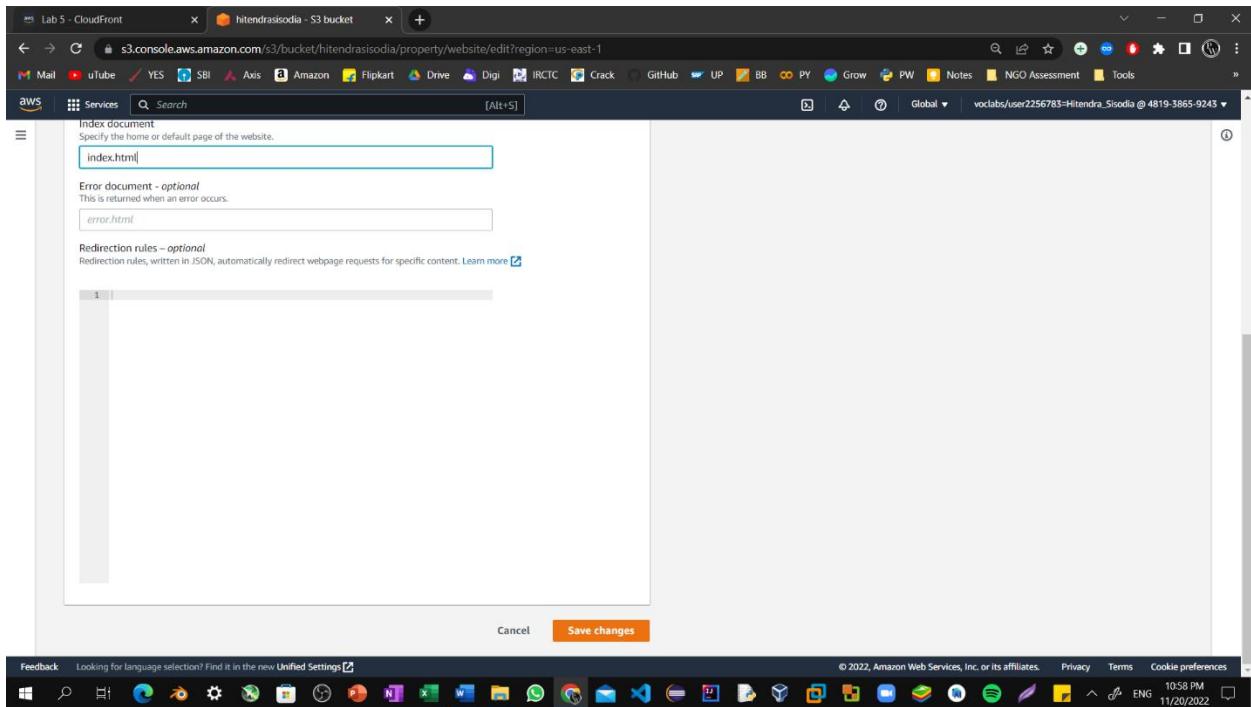
**Step17:** Select the Properties tab, and scroll down to the Static website hosting section. Choose Edit.

The screenshot shows the 'Properties' tab of the 'hitendrasisodia' bucket. The 'Static website hosting' section is expanded, showing the status as 'Disabled'. Other sections like 'Object Lock' and 'Requester pays' are also visible but not edited.

Step18: Select **Enable**. In the **Index document** text box, enter `index.html`



Step19: Select **Save changes**.



**Step20:** Scroll down to the **Static website hosting** section again, and copy the **Bucket website endpoint URL** to your clipboard.

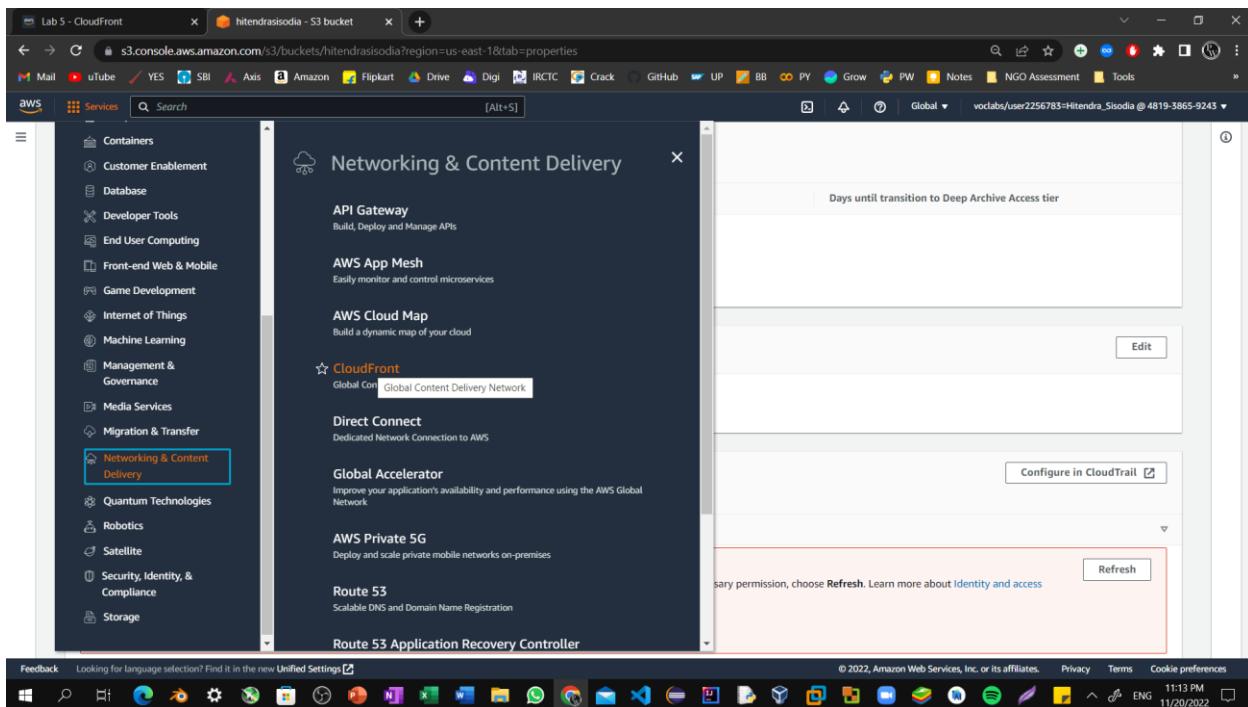
The screenshot shows the AWS S3 console for a bucket named 'hitendrasisodia'. In the 'Static website hosting' section, the 'Enabled' option is selected. Below it, the 'Bucket website endpoint' is listed as <http://hitendrasisodia.s3-website-us-east-1.amazonaws.com>. A red box highlights this URL.

**Step21:** Open a new tab in your web browser, paste the URL you just copied, and press **Enter**. The **Hello World** webpage should display. You have successfully hosted a static website using an S3 bucket!

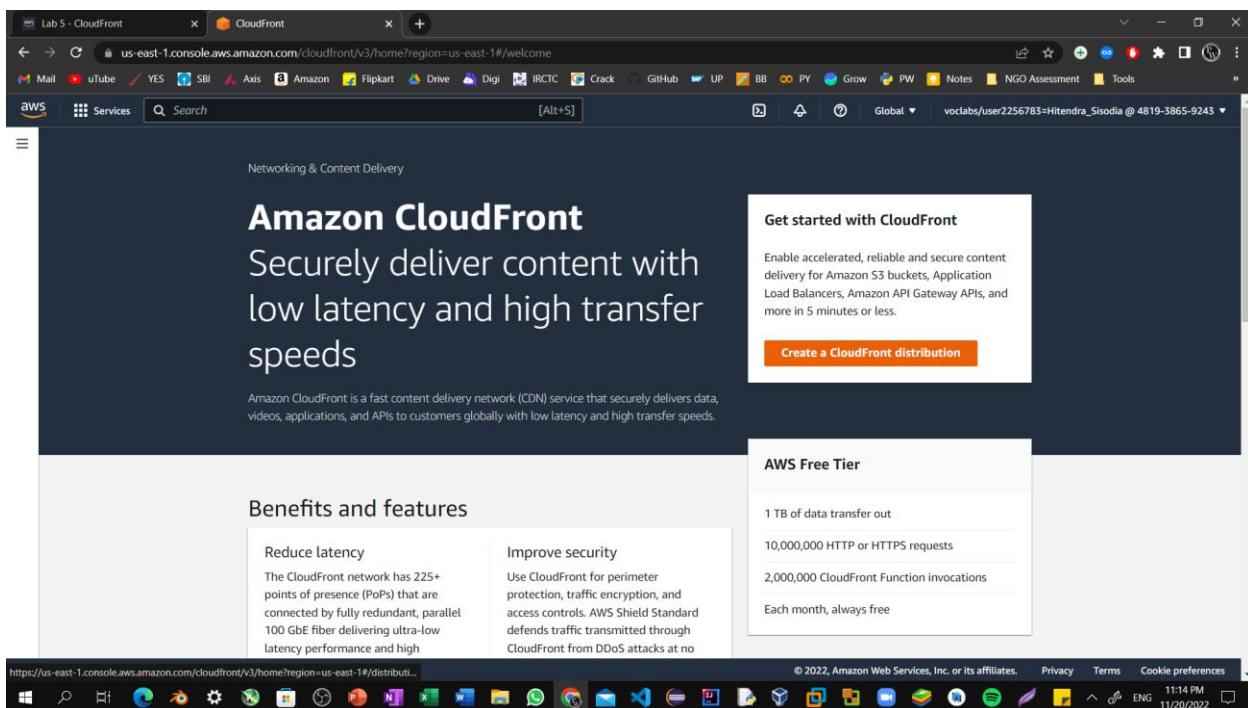
The screenshot shows a web browser window with the URL <http://hitendrasisodia.s3-website-us-east-1.amazonaws.com>. The page displays the text "Hello World. Take me to your leader." A red box highlights this text.



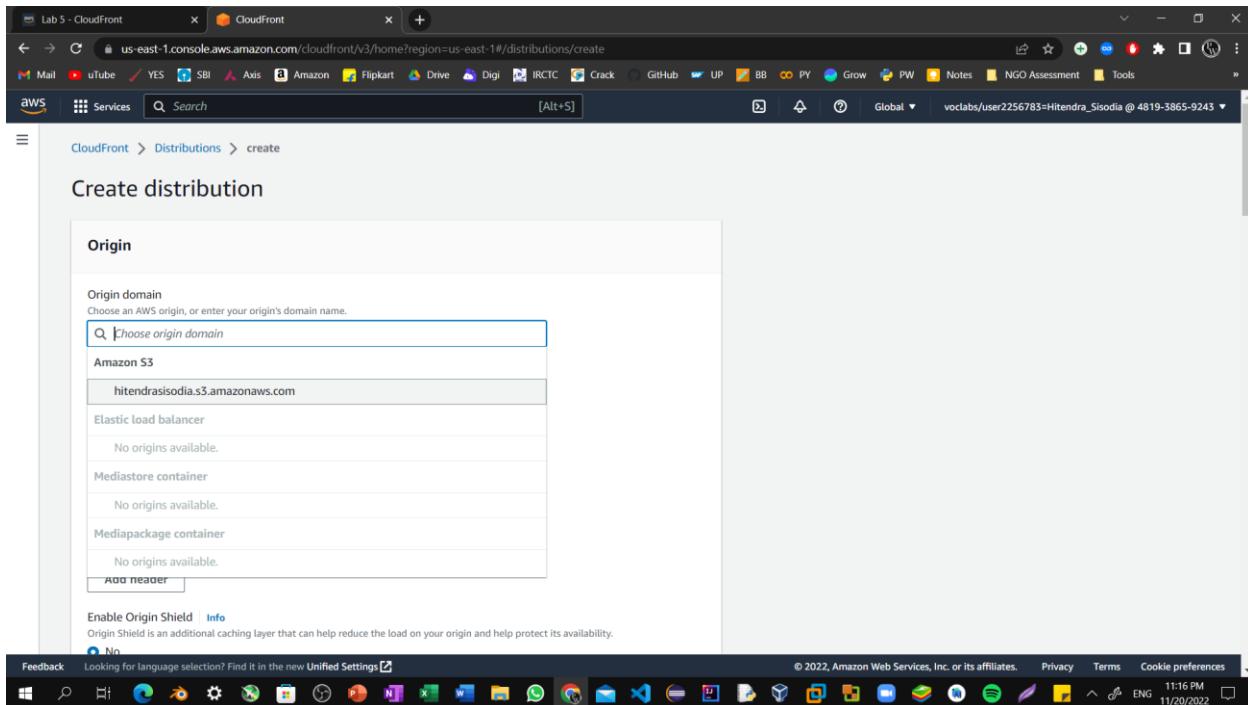
Step22: Choose the **Services** menu, locate the **Networking & Content Delivery** section, and choose **CloudFront**.



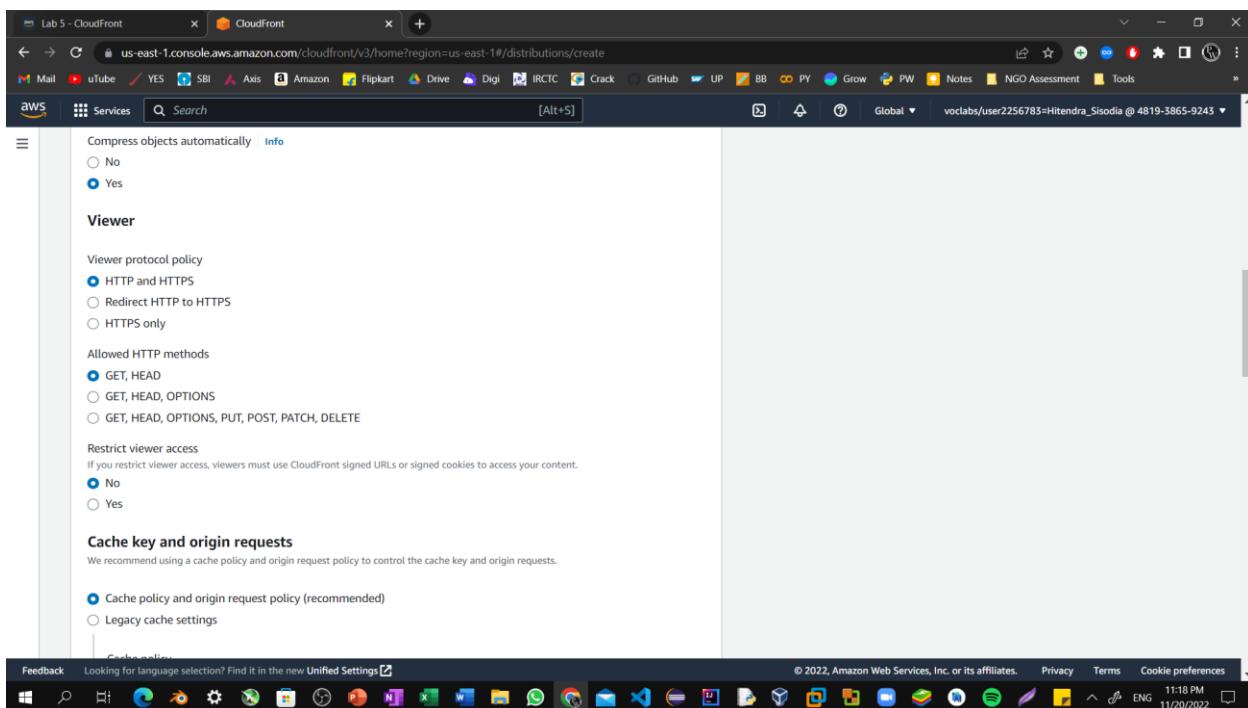
Step23: Choose **Create Distribution**.



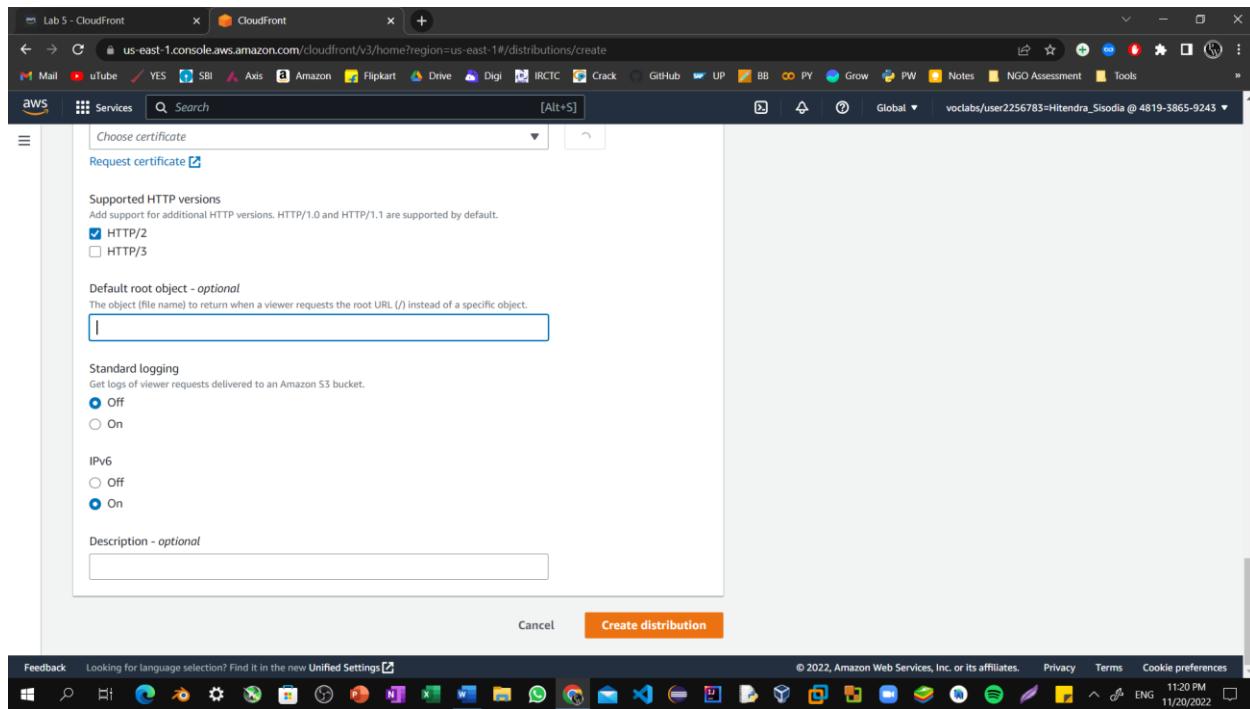
Step24: Choose the text box next to **Origin Domain Name** and select the endpoint from your S3 bucket.



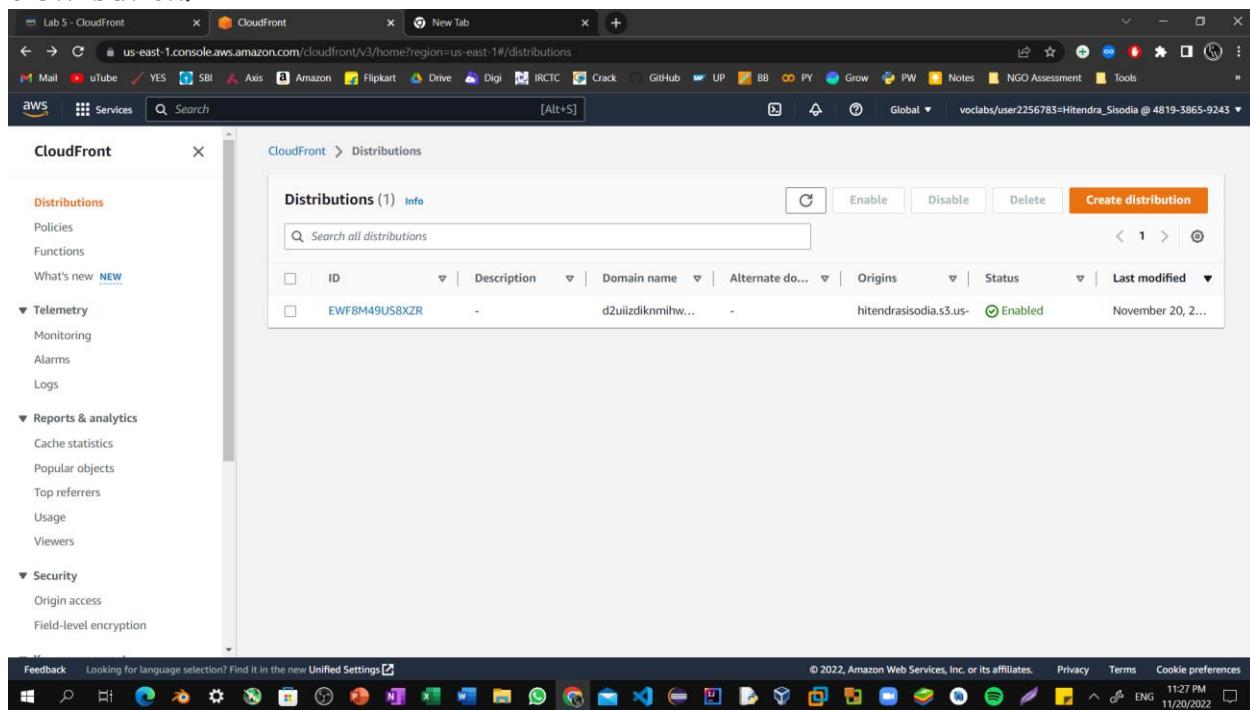
Step25: For **Viewer Protocol Policy**, ensure that **HTTP and HTTPS** is selected.



Step26: Scroll to the bottom of the page and select **Create Distribution**.

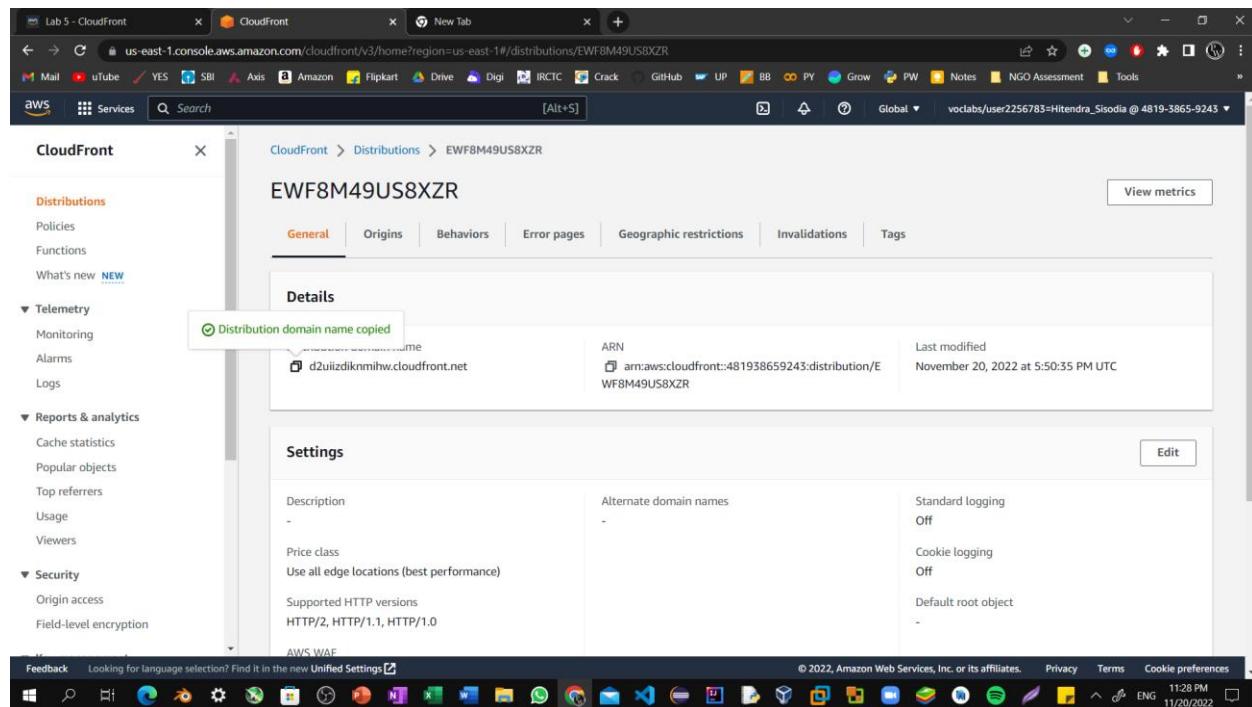


Step27: A new CloudFront distribution displays in the distributions list.  
The **Status** will say *In Progress* until your website has been distributed. This may take up to 20 minutes. When the **Status** says *Deployed*, you can test your distribution.

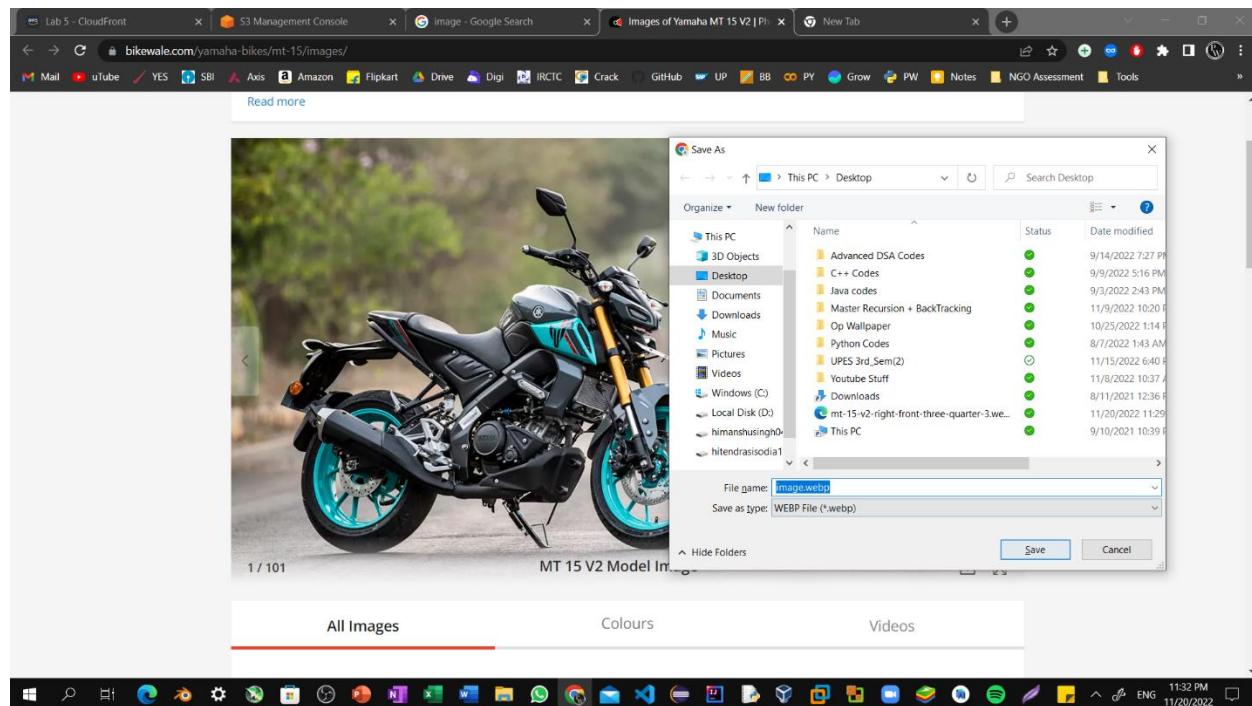


## Lab 12: Using CloudFront As a CDN For A Website

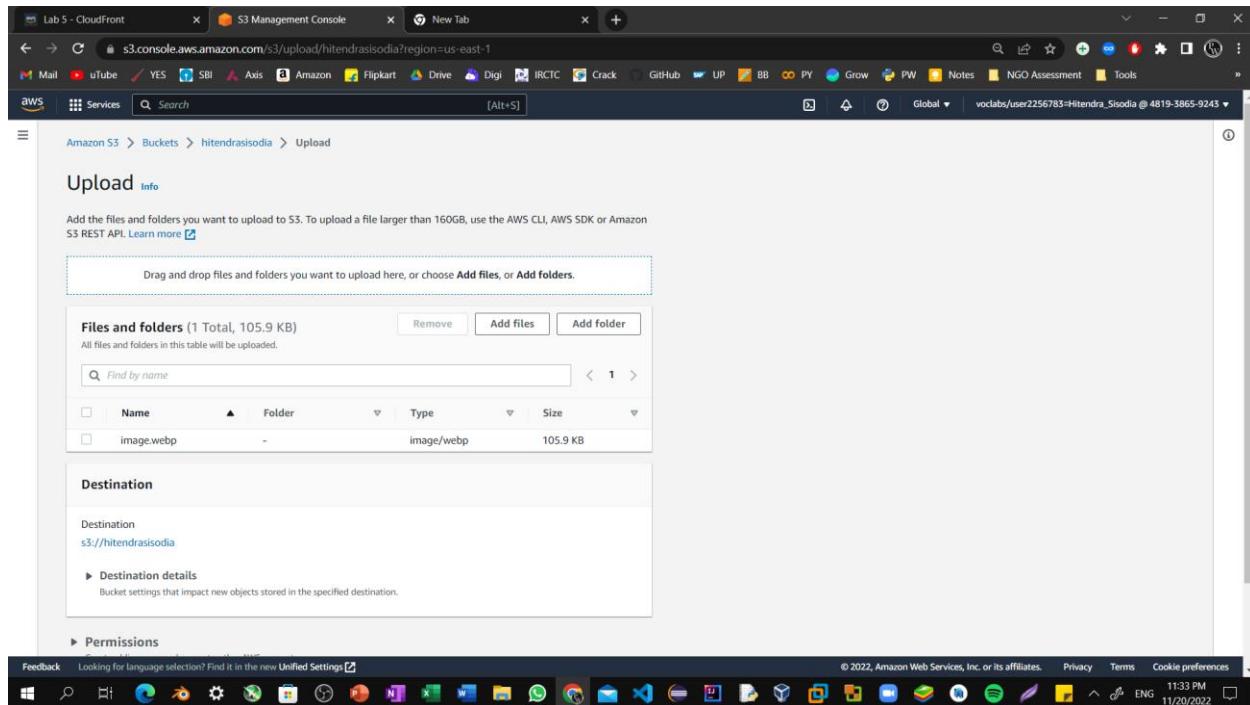
Step28: Copy the Domain Name value for your distribution and save it to a text editor to use in a later step.



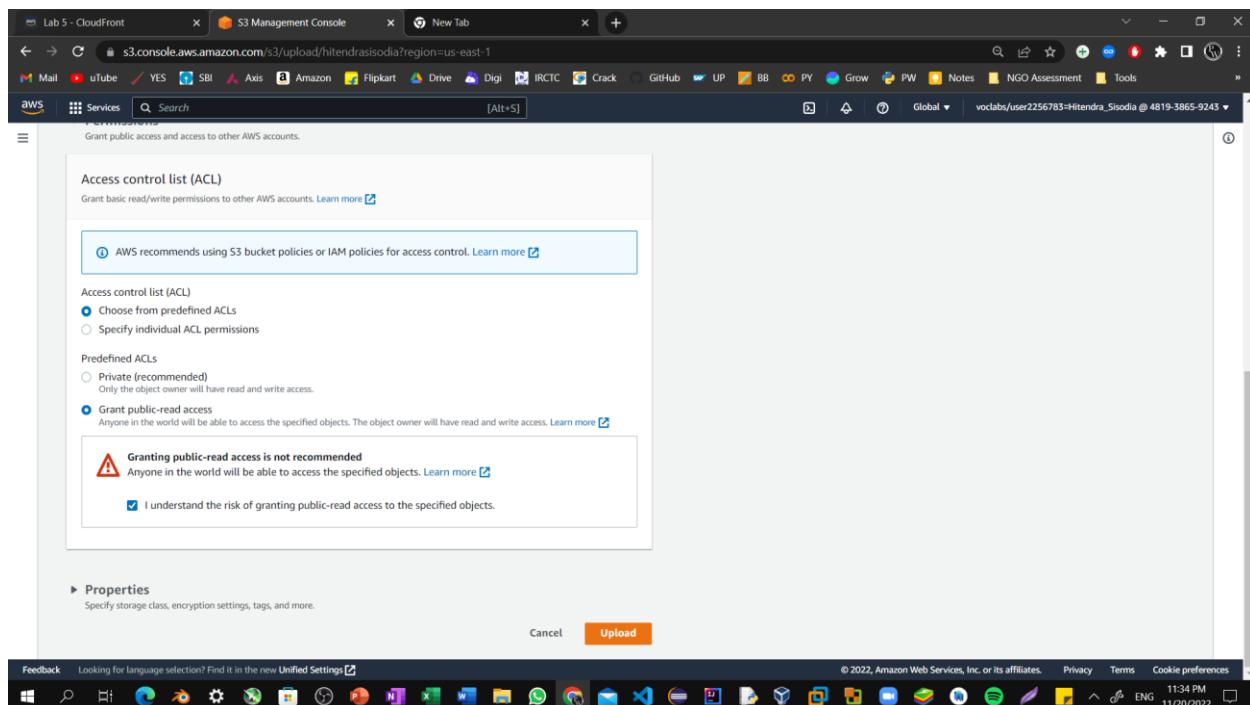
Step29: Create a new HTML file to test the distribution. Find and download an image from the internet.



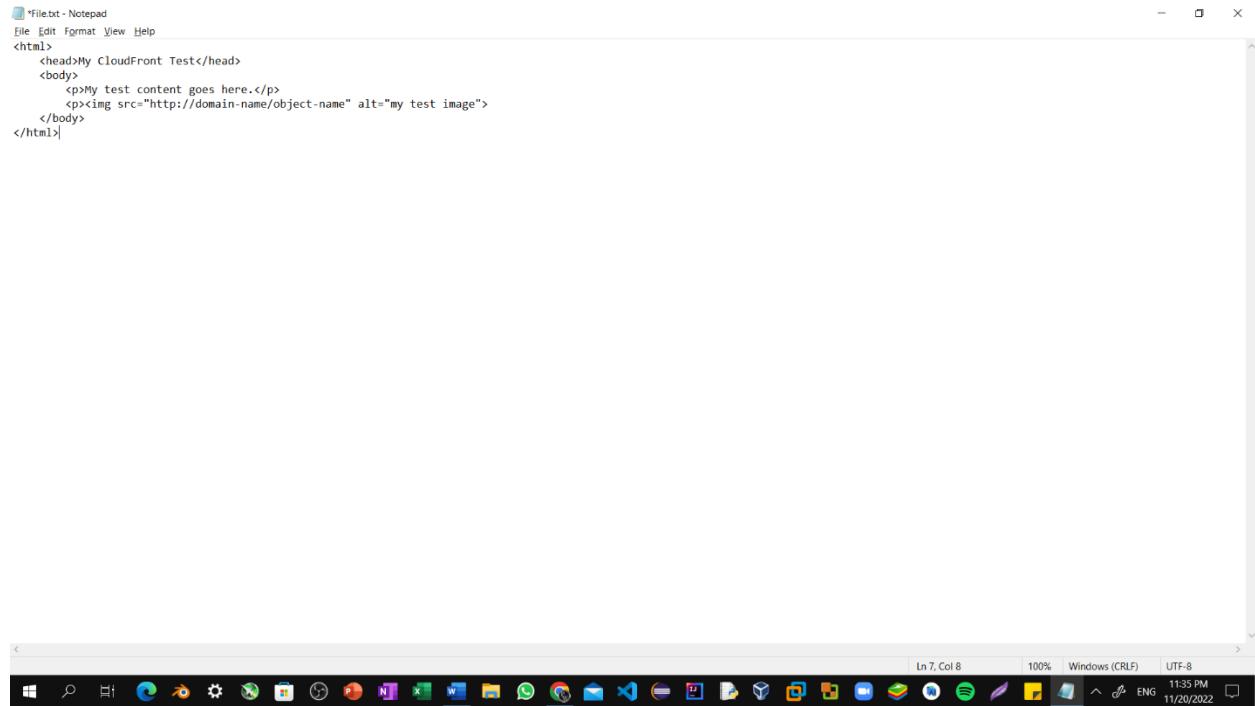
Step30: Navigate to your S3 bucket and upload the image file to it.



Step31: Making sure to grant public access as you did when uploading the HTML file earlier in this lab.

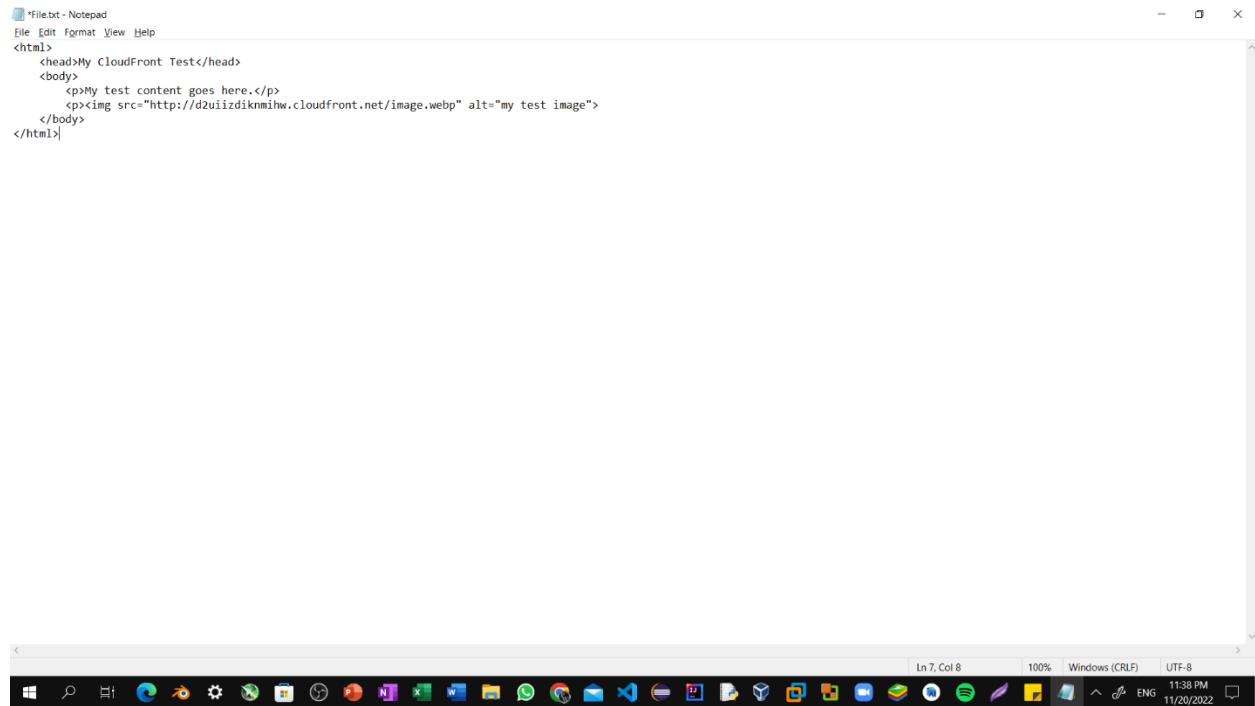


Step32: Create a new text file using Notepad and copy the following text into it.



```
<html>
<head>My CloudFront Test</head>
<body>
    <p>My test content goes here.</p>
    <p></p>
</body>
</html>
```

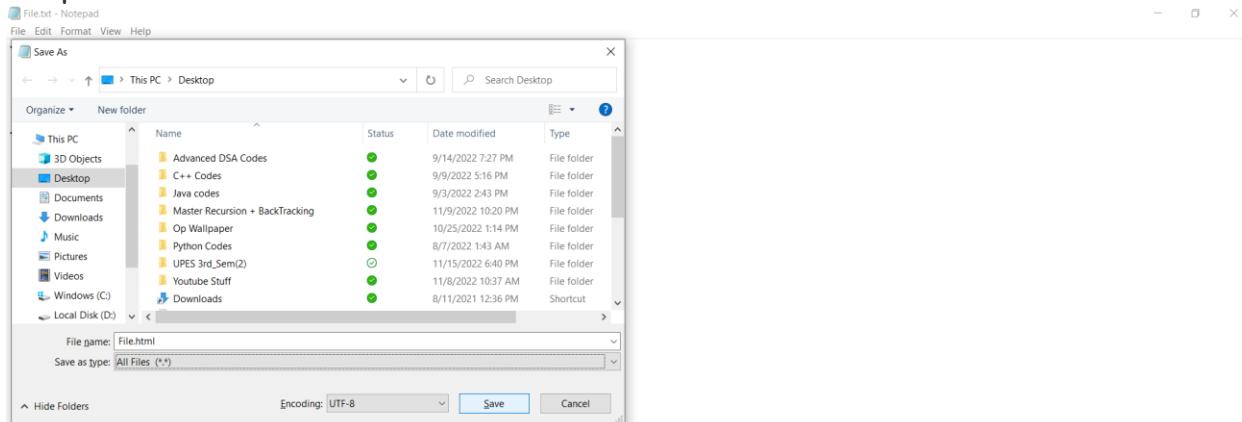
Step33: Replace **domain-name** with the domain name that you copied earlier for your CloudFront distribution. Replace **object-name** with the file name of the picture file that you uploaded to your S3 bucket.



```
<html>
<head>My CloudFront Test</head>
<body>
    <p>My test content goes here.</p>
    <p></p>
</body>
</html>
```

## Lab 12: Using CloudFront As a CDN For A Website

Step34: Save the text file with an HTML extension.



Step35: Use an internet browser to open the HTML file that you just created. If the image that you uploaded shows, your CloudFront distribution was successful. If not, repeat the lab.

