

## **Experiment No. 01**

---

**Aim:** Introduction and overview of cloud computing

**Theory:**

**Introduction:**

Cloud computing is a model of computing that provides on-demand access to a shared pool of computing resources, including servers, storage, applications, and services. These resources can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing enables users to access applications and data from anywhere, on any device, and at any time, if they have an internet connection. Cloud computing is a popular and rapidly growing technology that is changing the way organizations manage their computing resources.

**Overview:**

Cloud computing can be categorized into three types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). IaaS provides users with access to virtualized computing resources, such as servers, storage, and networking, which can be managed and configured by the user. PaaS provides users with a platform on which they can develop and deploy their applications, without having to worry about the underlying infrastructure. SaaS provides users with access to software applications that are hosted and managed by a third-party provider, eliminating the need for users to install or maintain the software themselves. Cloud computing offers several benefits, including:

- **Scalability:** Cloud computing resources can be scaled up or down as per the user's requirements, providing flexibility and cost savings.
- **Cost savings:** Cloud computing eliminates the need for users to invest in expensive hardware and software infrastructure, as well as the associated maintenance costs.
- **Accessibility:** Cloud computing resources can be accessed from anywhere, on any device, if there is an internet connection.
- **Reliability:** Cloud computing providers offer high availability and redundancy, ensuring that users' applications and data are always available.
- **Security:** Cloud computing providers invest heavily in security measures to ensure that users' applications and data are secure and protected.

## **Origin of Cloud Computing:**

The concept of cloud computing can be traced back to the 1960s, when mainframe computers were first introduced. However, the term "cloud computing" was not coined until the late 1990s. The development of virtualization technology in the 2000s enabled cloud computing to become a reality. Amazon Web Services (AWS) launched its Elastic Compute Cloud (EC2) in 2006, which was the first widely adopted cloud computing platform.

## **Characteristics of Cloud Computing:**

Cloud computing is characterized by several key features, including:

- **On-demand self-service:** Users can provision and manage cloud resources without requiring human interaction with the service provider.
- **Broad network access:** Cloud resources can be accessed from anywhere, on any device, with an internet connection.
- **Resource pooling:** Cloud resources are shared among multiple users, providing economies of scale and cost savings.
- **Rapid elasticity:** Cloud resources can be scaled up or down quickly and easily, based on user demand.
- **Measured service:** Cloud resources are measured and billed based on usage, providing cost transparency and predictability.

## **Advantages of Cloud Computing:**

- I. **Collaboration:** Cloud computing allows multiple users to collaborate on documents and projects in real-time, improving productivity and teamwork.
- II. **Disaster recovery:** Cloud computing providers offer backup and disaster recovery services, ensuring that users' data is protected in the event of a disaster or outage.
- III. **Innovation:** Cloud computing providers offer a range of innovative services and technologies, such as artificial intelligence and machine learning, that can help businesses stay competitive and innovative.

## **Disadvantages of Cloud Computing:**

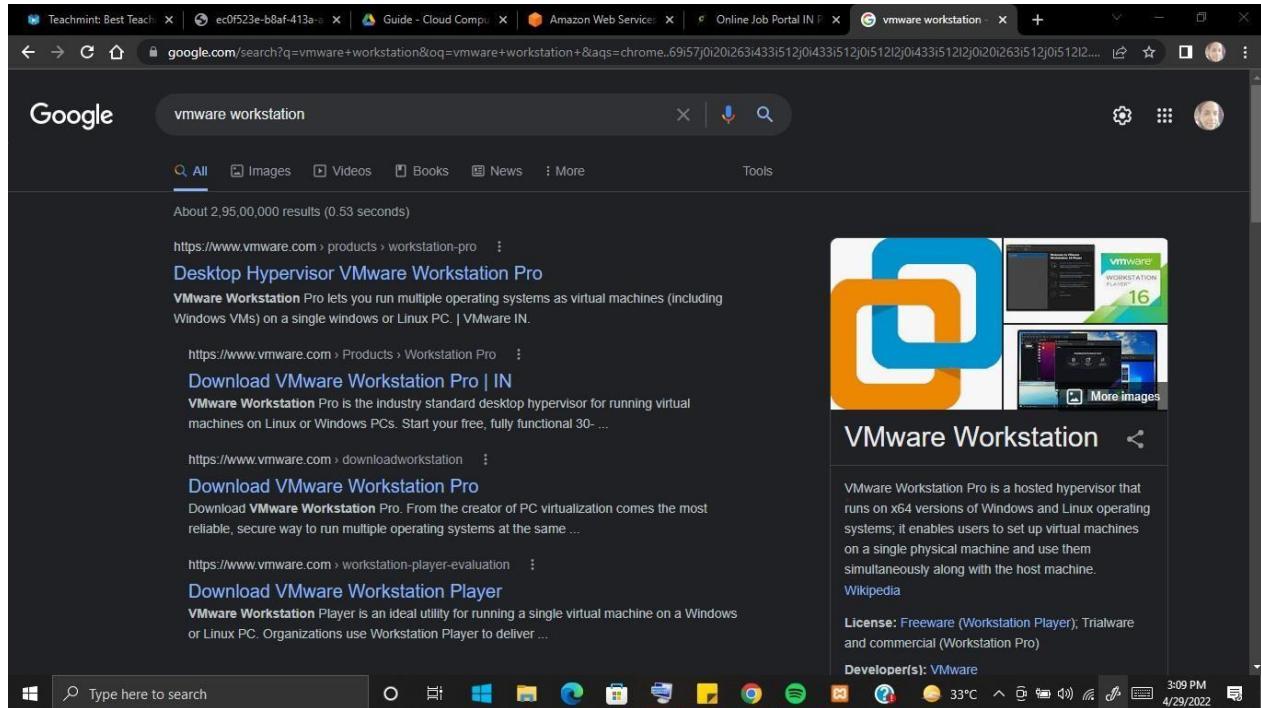
Cloud computing also has several potential disadvantages, including:

- I. **Dependency:** Users become dependent on the cloud provider for their computing resources, which can be a concern for some organizations.
- II. **Security risks:** Cloud computing providers are responsible for the security of their infrastructure, but users are responsible for the security of their applications and data.
- III. **Limited control:** Users have limited control over the underlying infrastructure, which can be a concern for some organizations.
- IV. **Downtime:** Cloud computing providers may experience downtime or outages, which can affect users' access to their applications and data.
- V. **Internet connectivity:** Users require a reliable internet connection to access cloud computing resources, which may not be available in all locations.

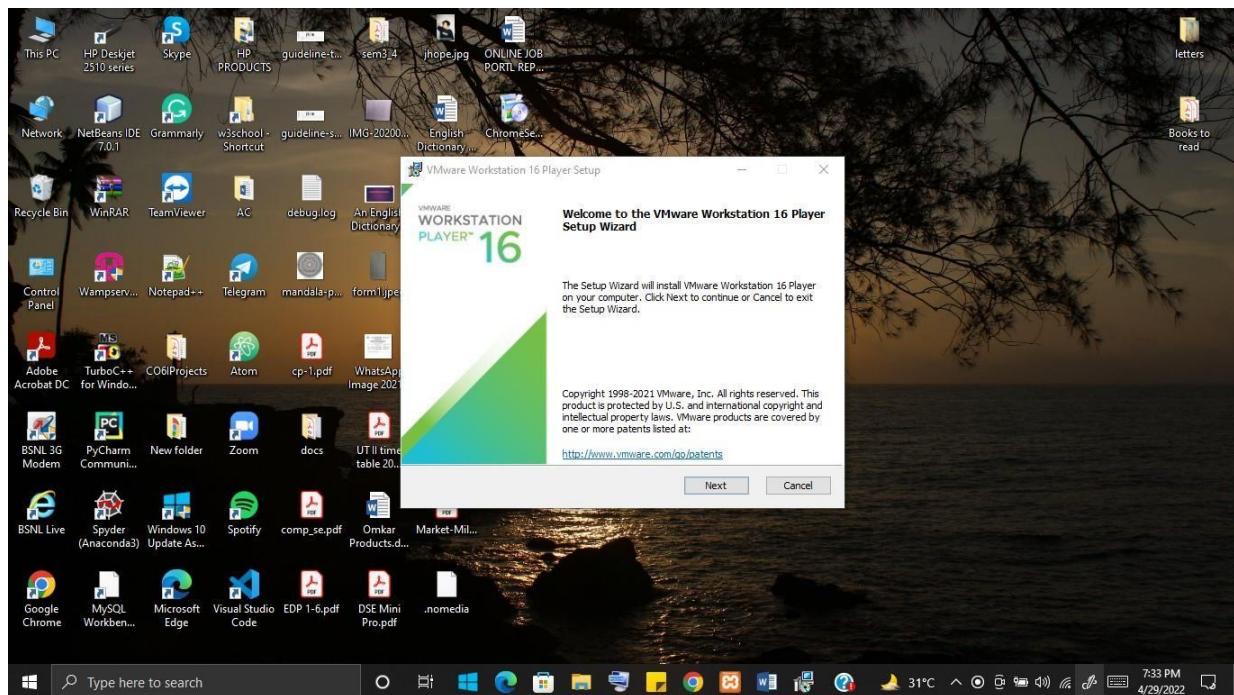
## Experiment No. 02

**Aim :** To study and implement Hosted Virtualization using VirtualBox& KVM.

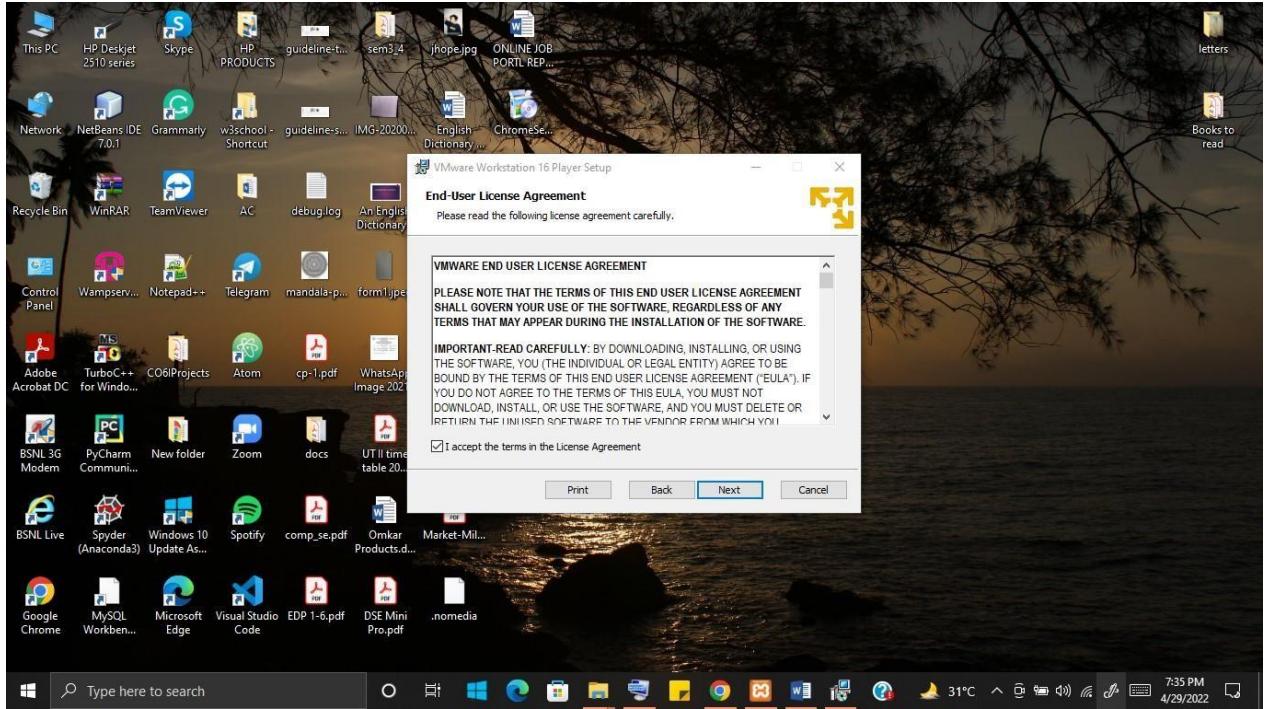
Step 1:



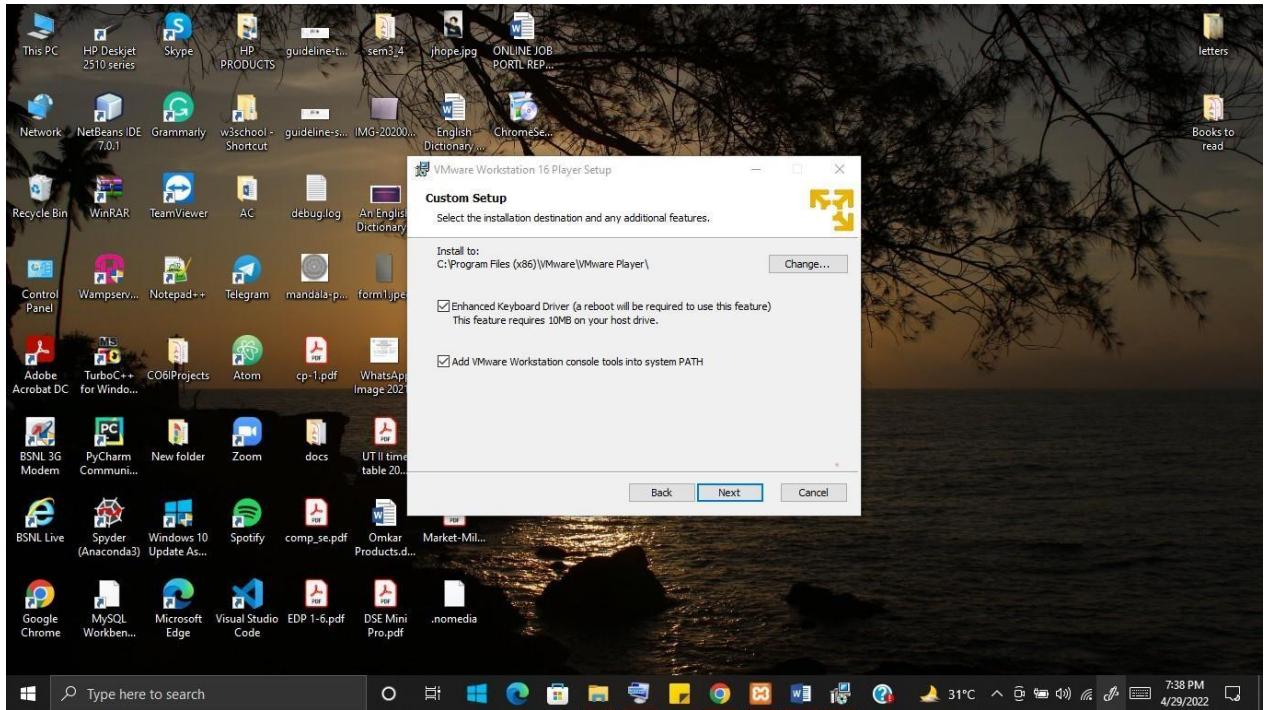
Step 2:



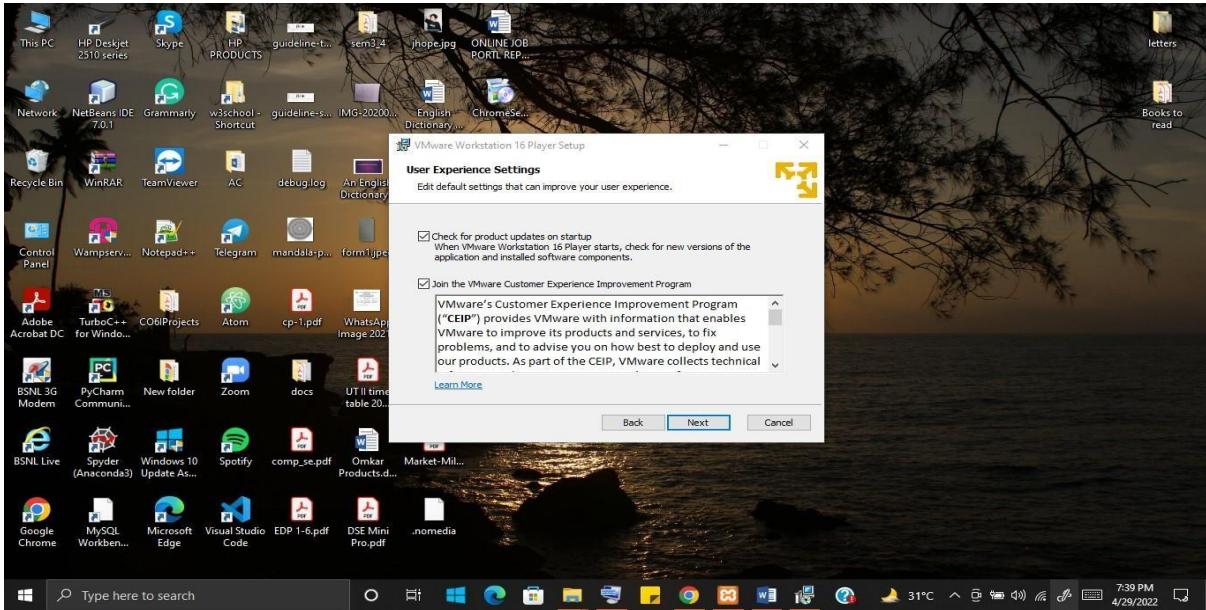
### Step 3:



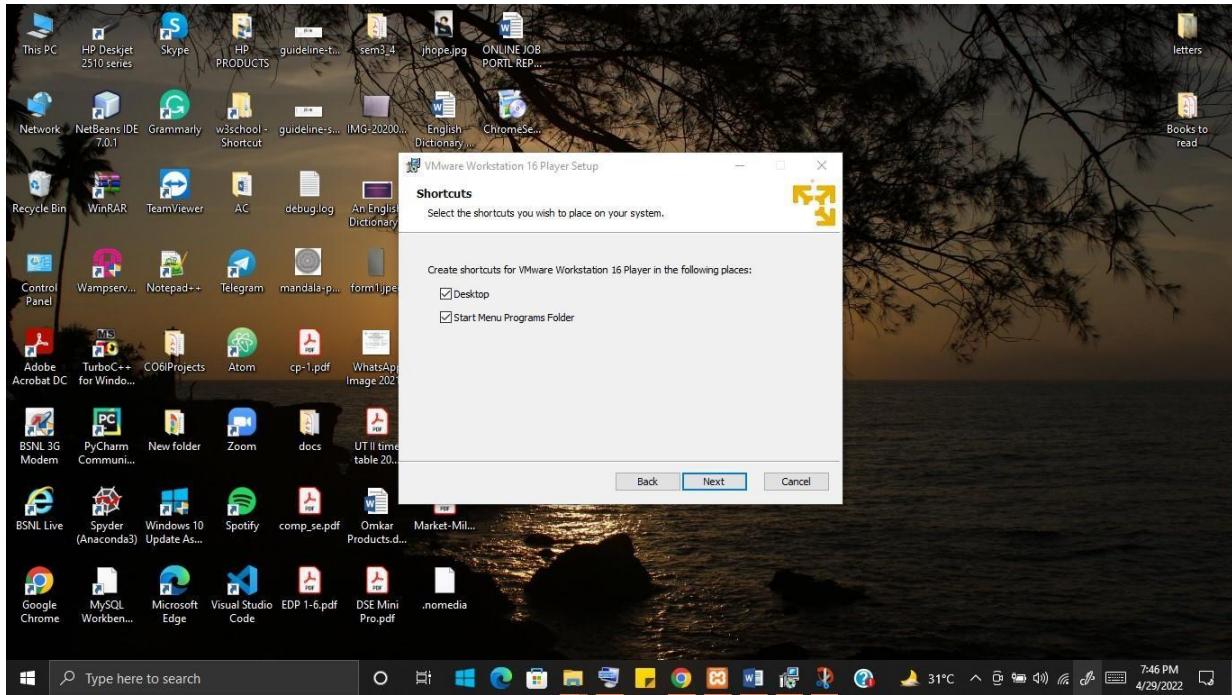
### Step 4:

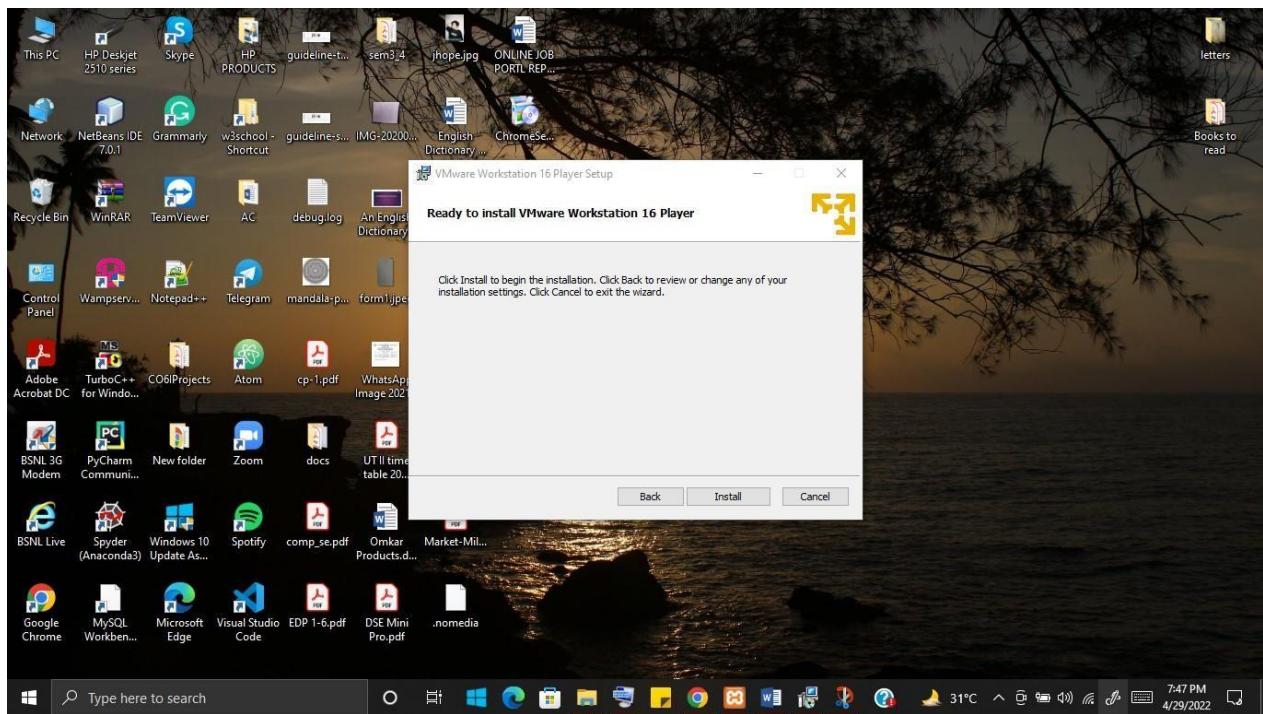


## Step 5:

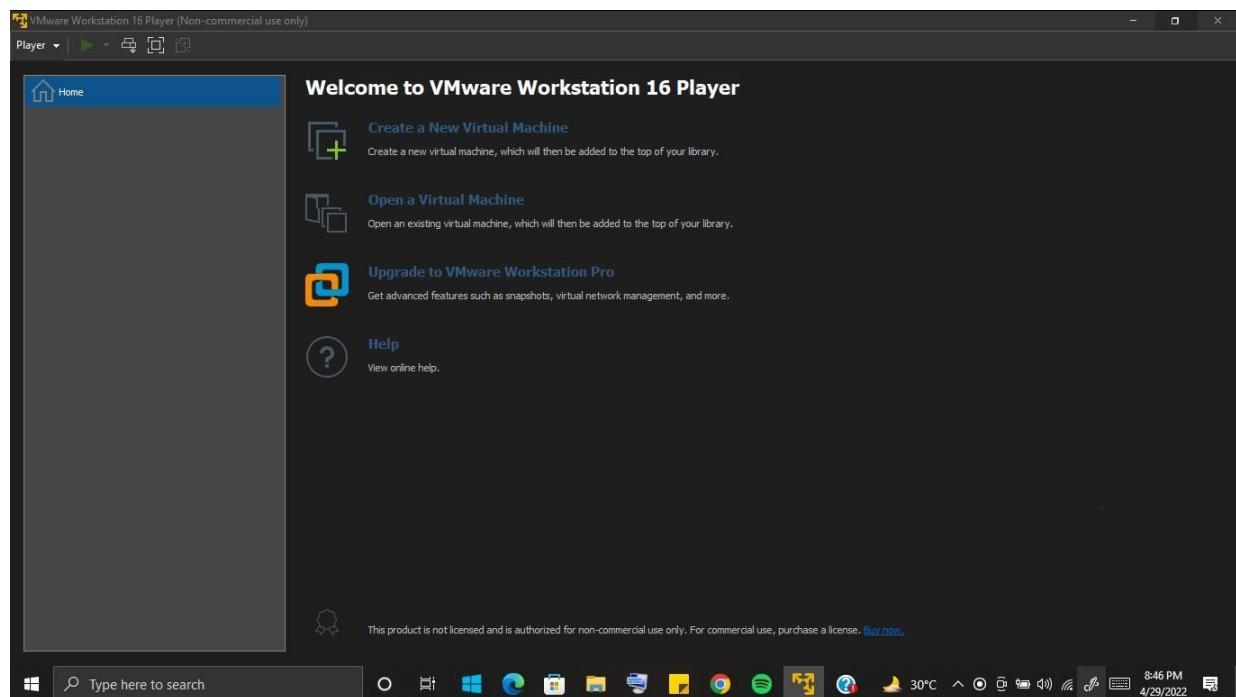


## Step 6:

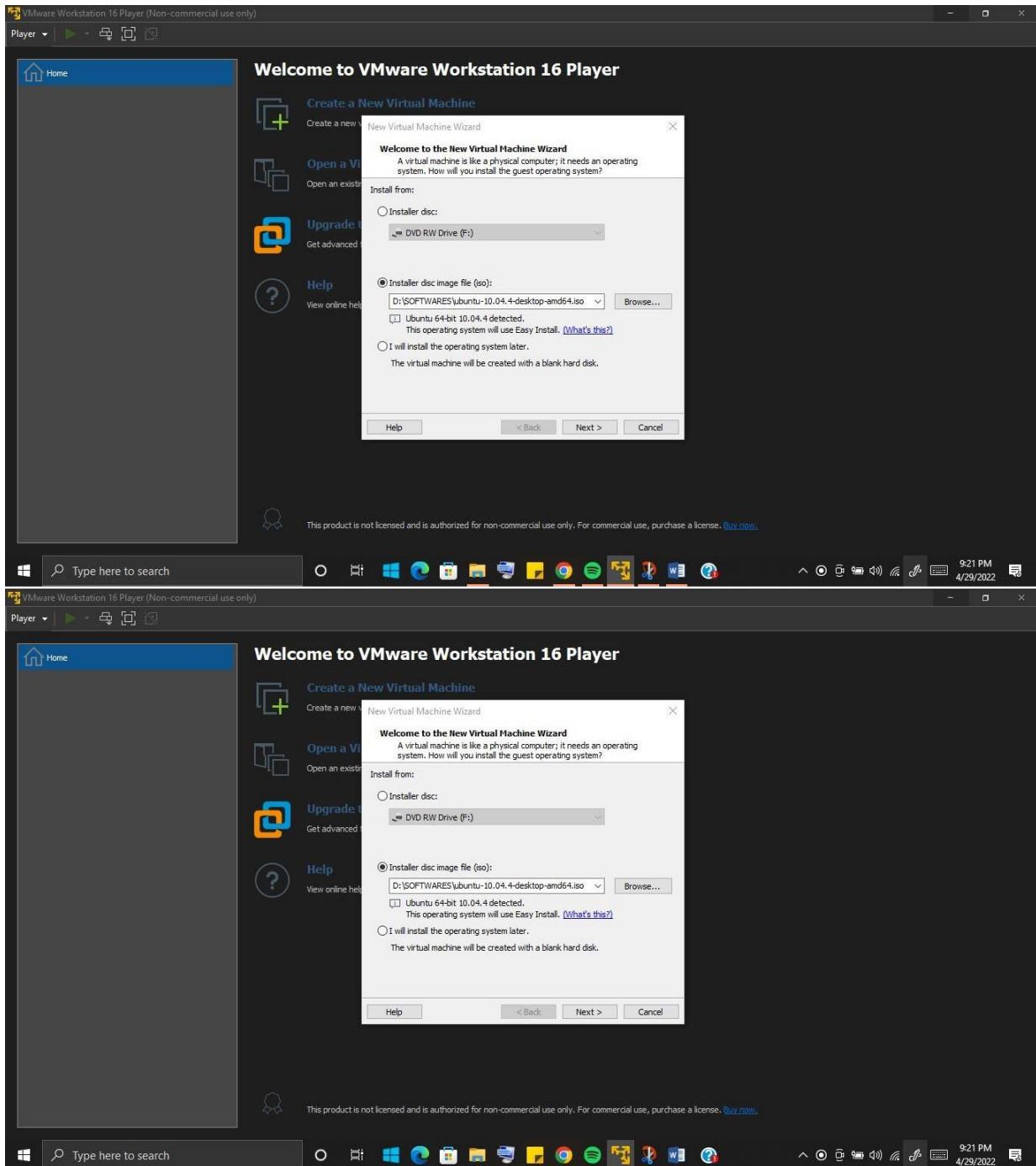




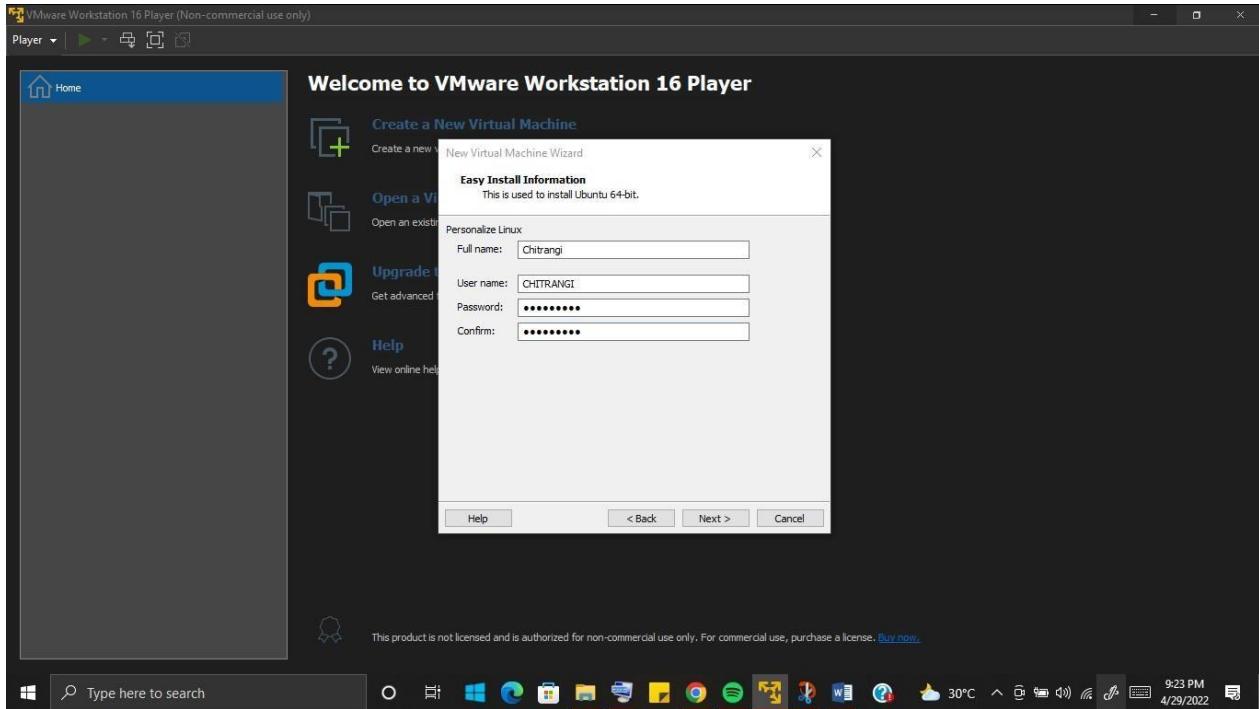
## Step 7:



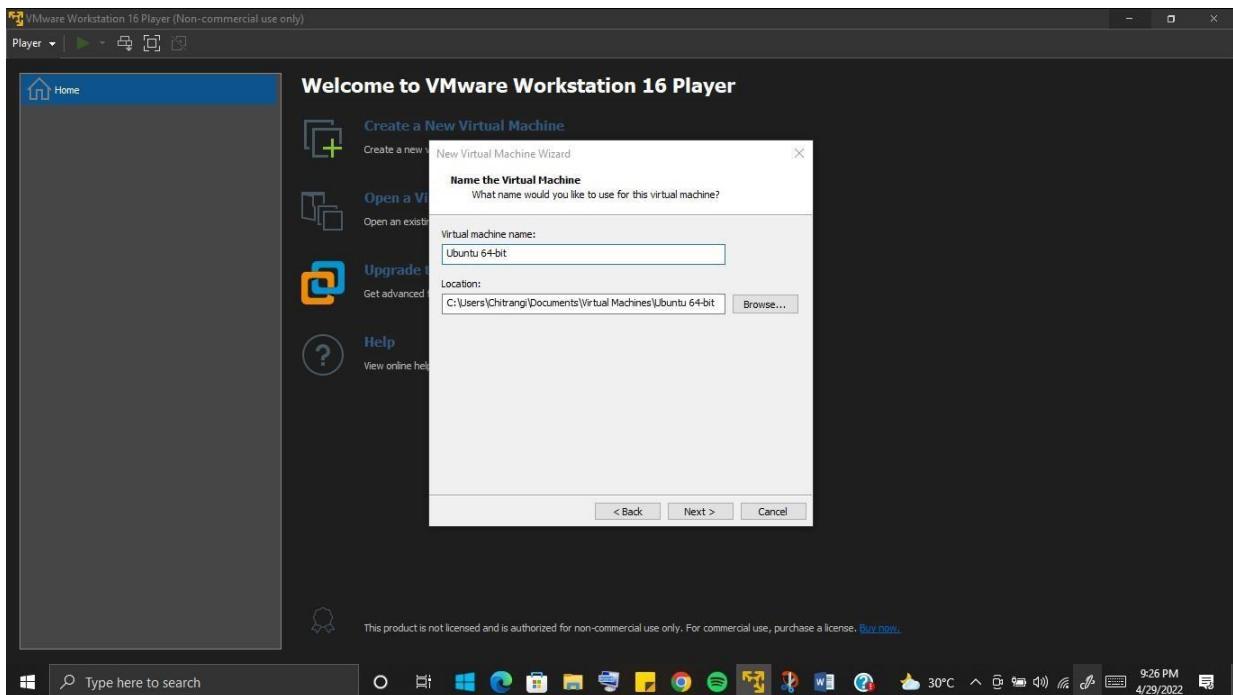
## Step 8:



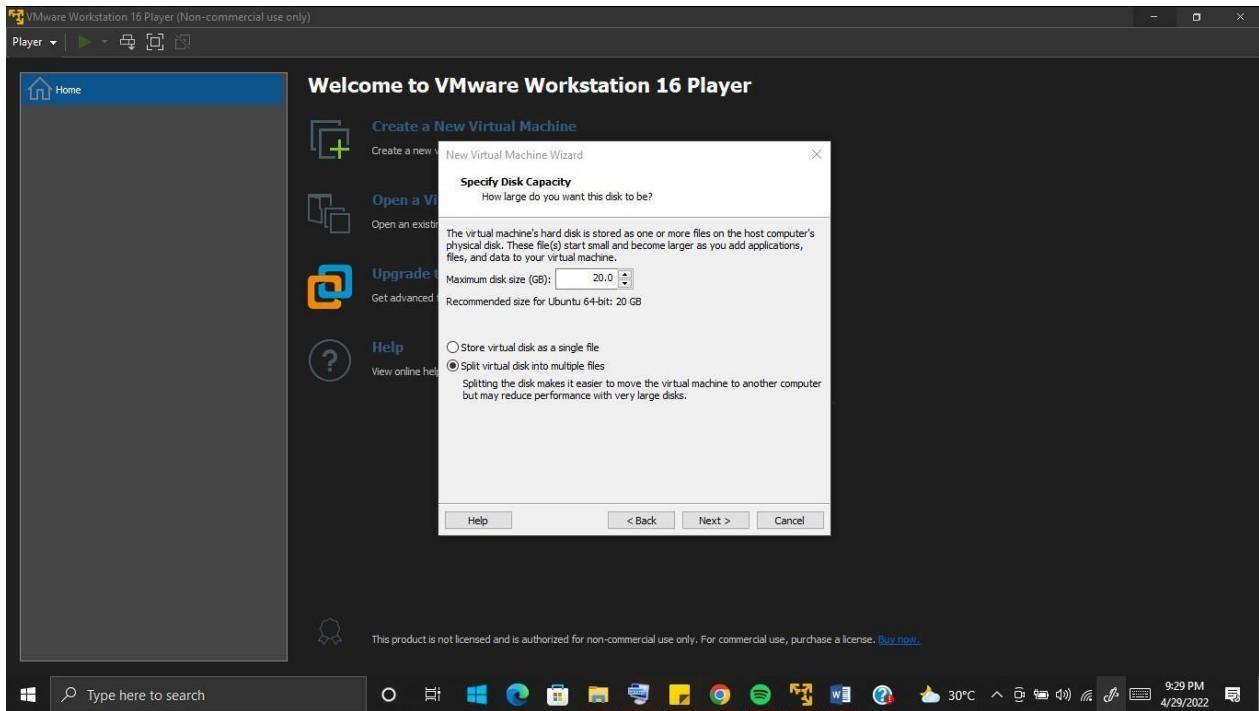
## Step 9:



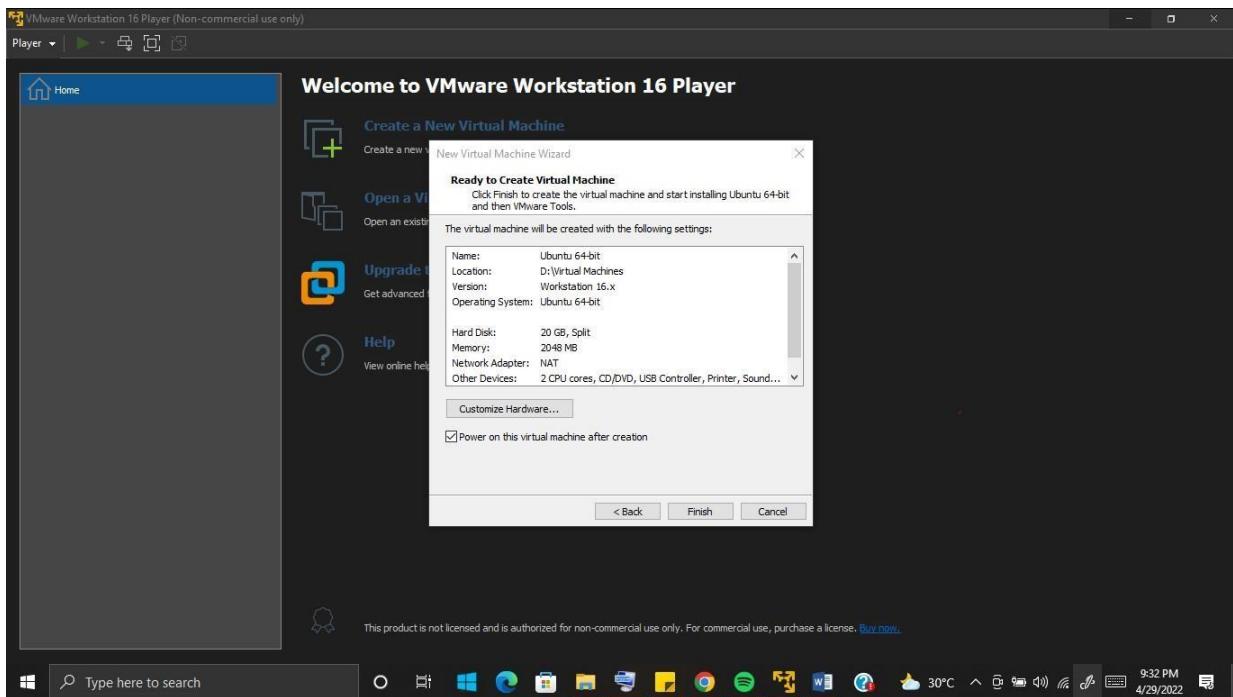
## Step 10:



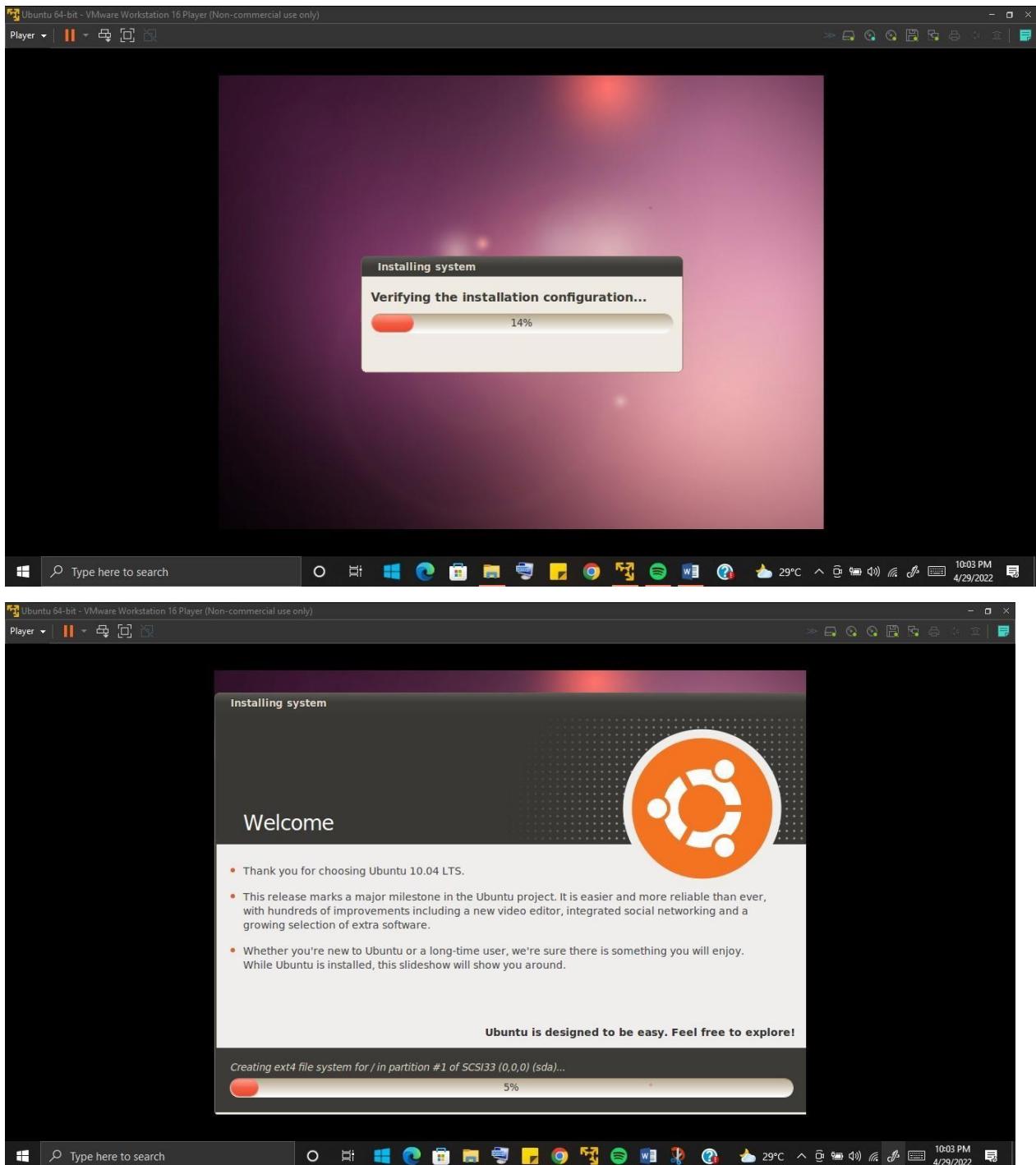
## Step 11:



## Step 12:



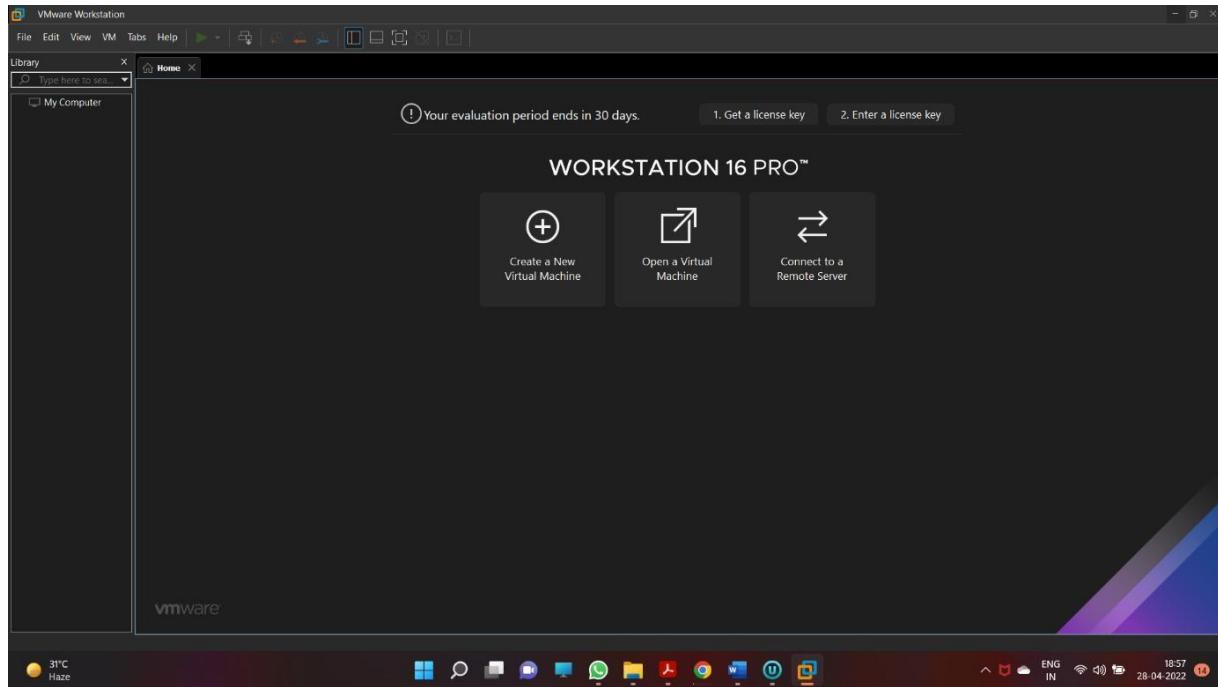
## Step 13:



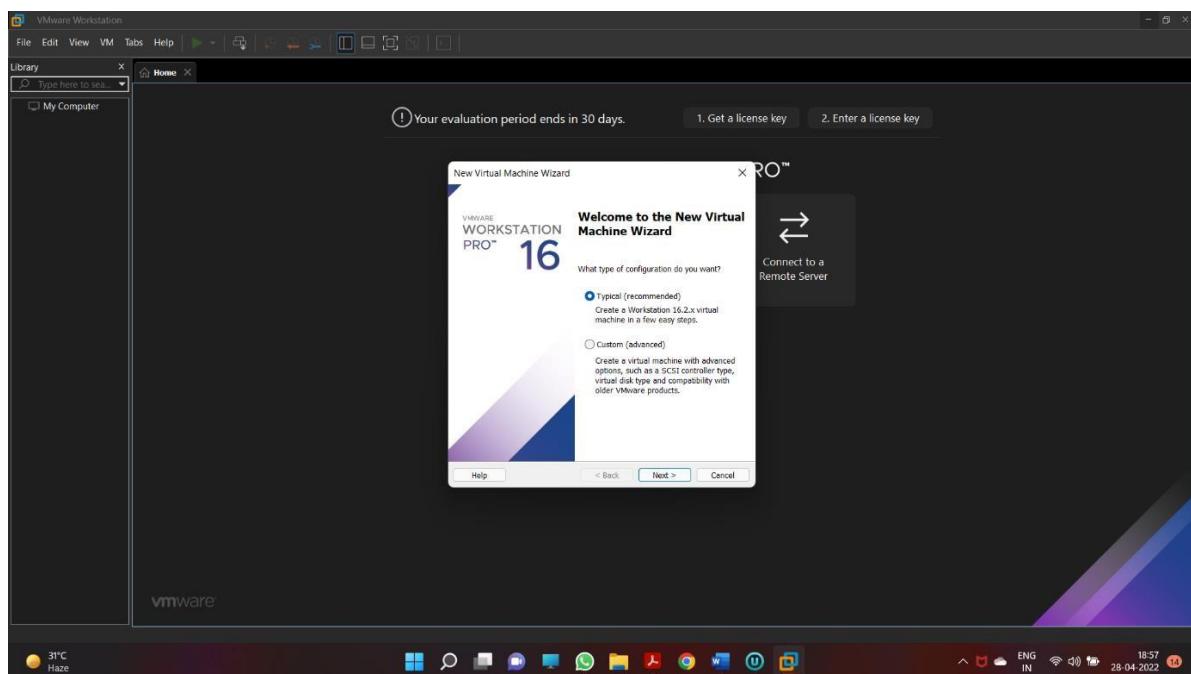
## EXPERIMENT NO 3

**Aim** - To study and Implement Bare-metal Virtualization using Xen, HyperV orVMware Esxi

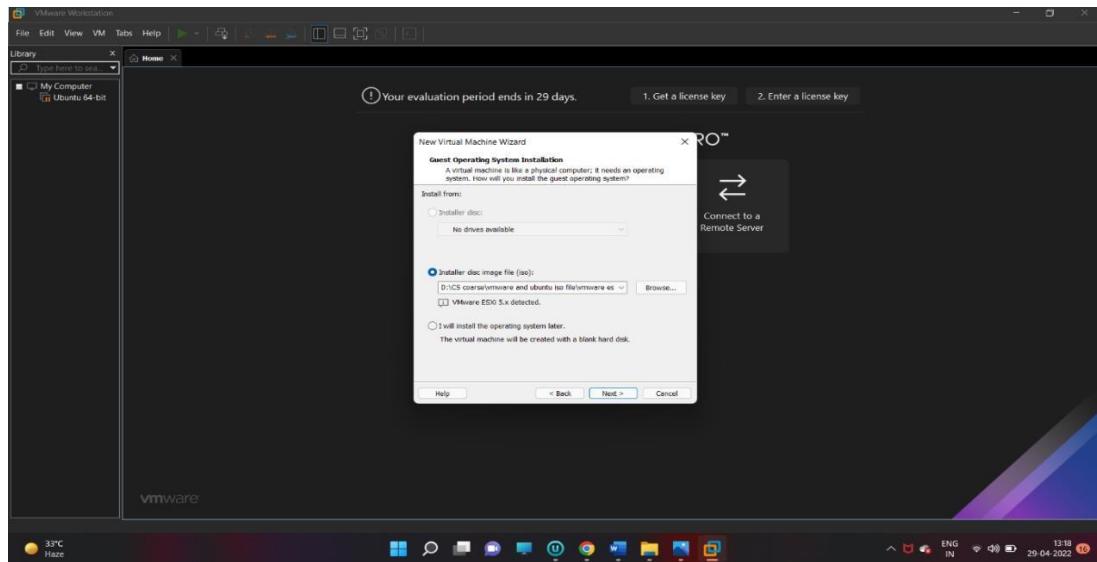
Step 1- Open VMware Workstation



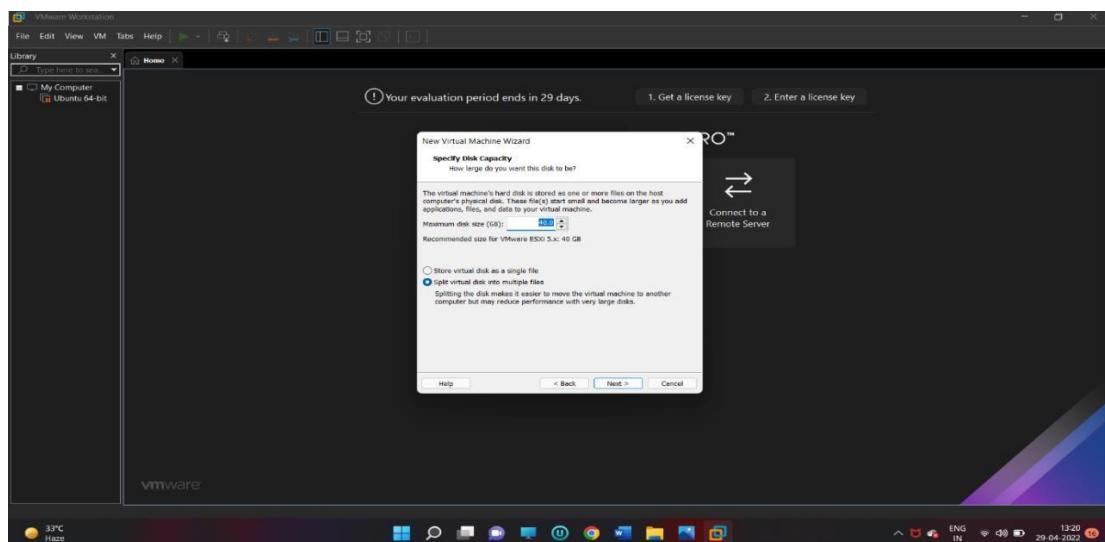
Step 2 – Click create Virtual Machine.



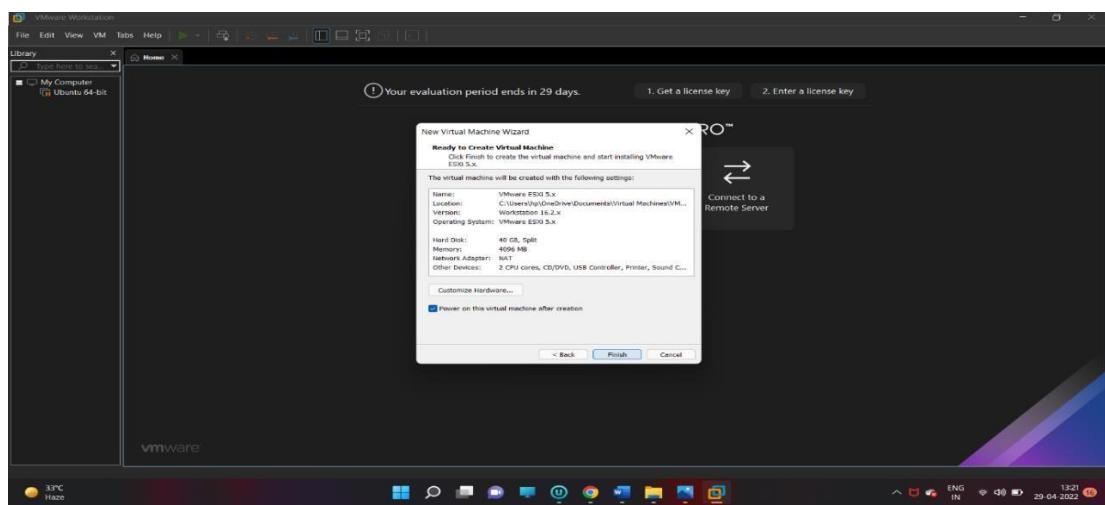
### Step 3 – Select vmware4 ESXI file location.



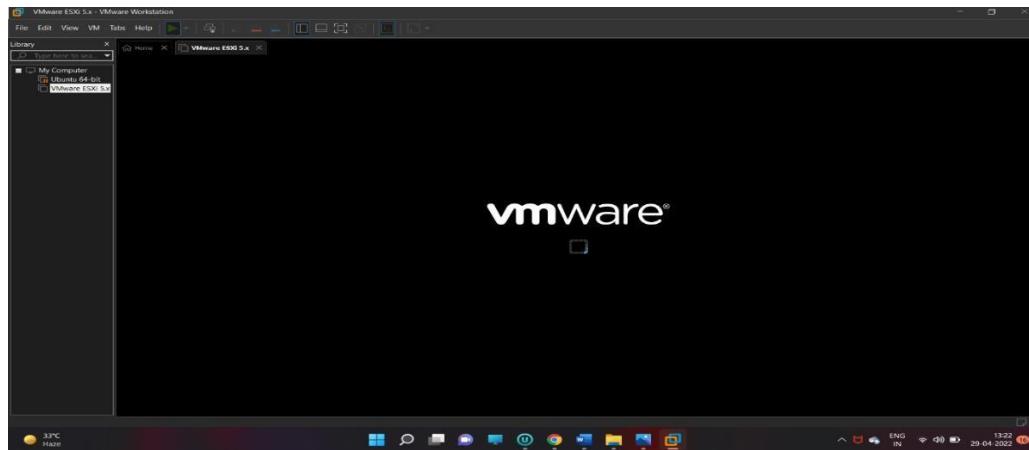
### Step 4 – Specify disk capacity



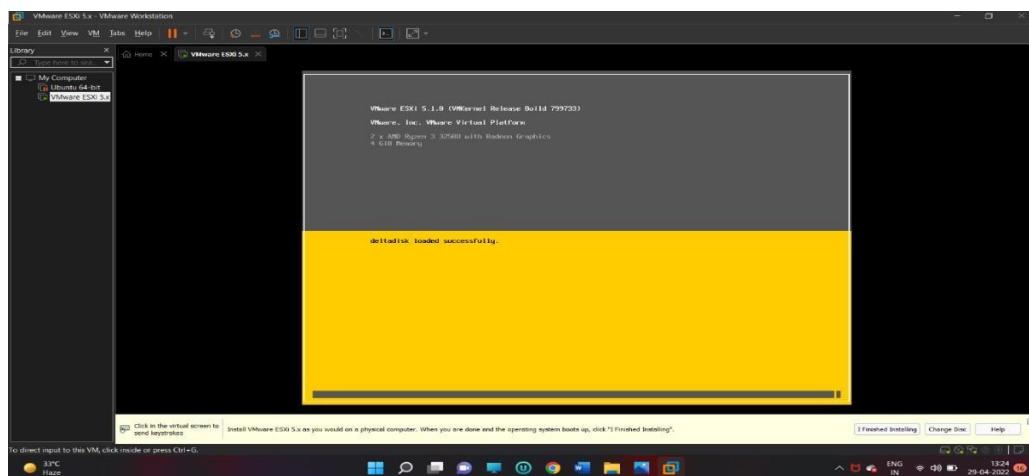
### Step 5 – Customized Hardware click finish .



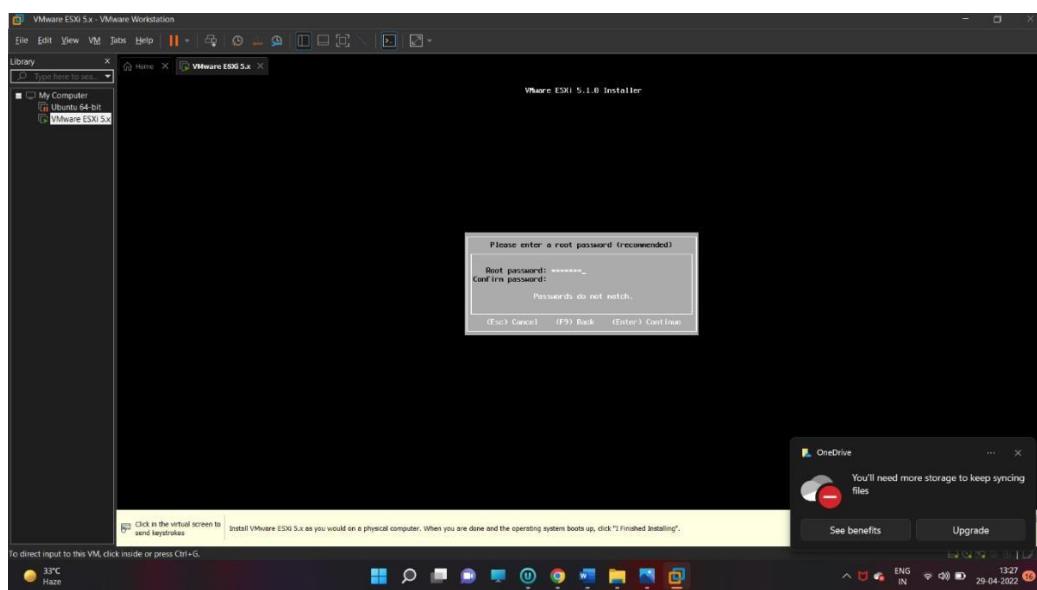
VMware instance created



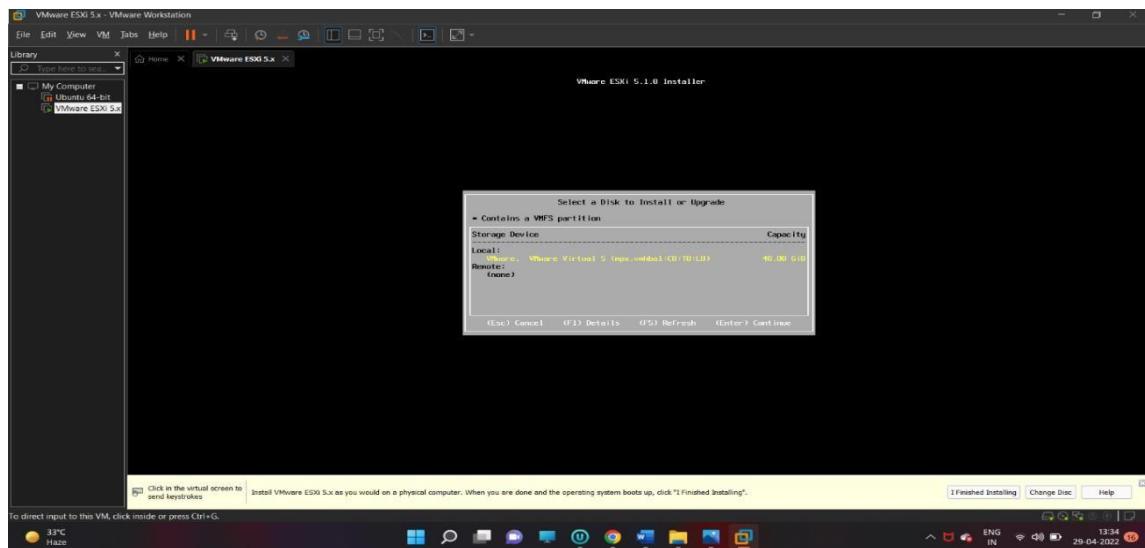
Step 6- Press F10 to install.



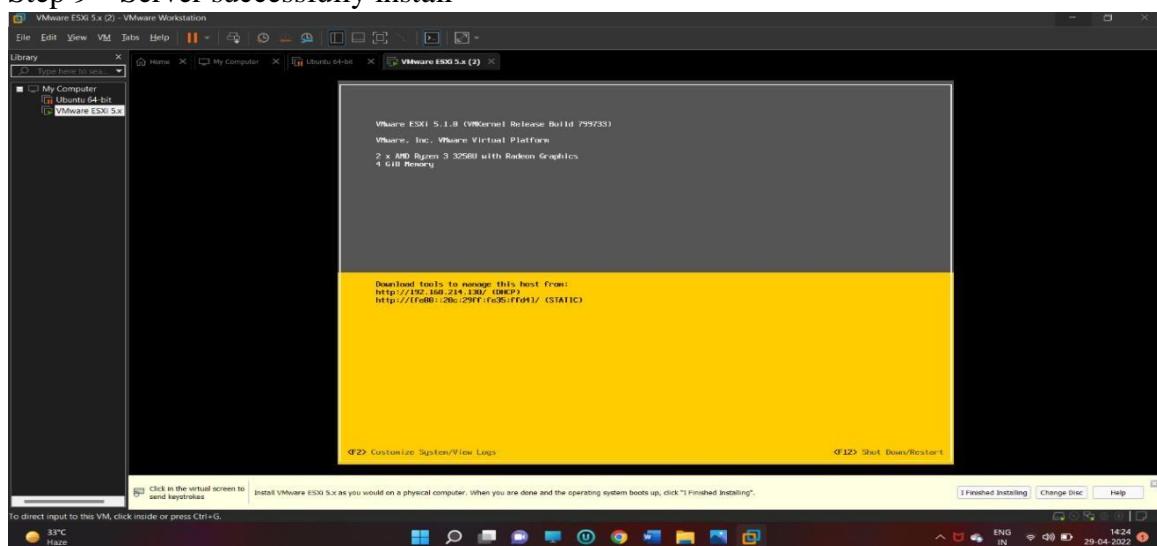
Step 7 – Create root password.



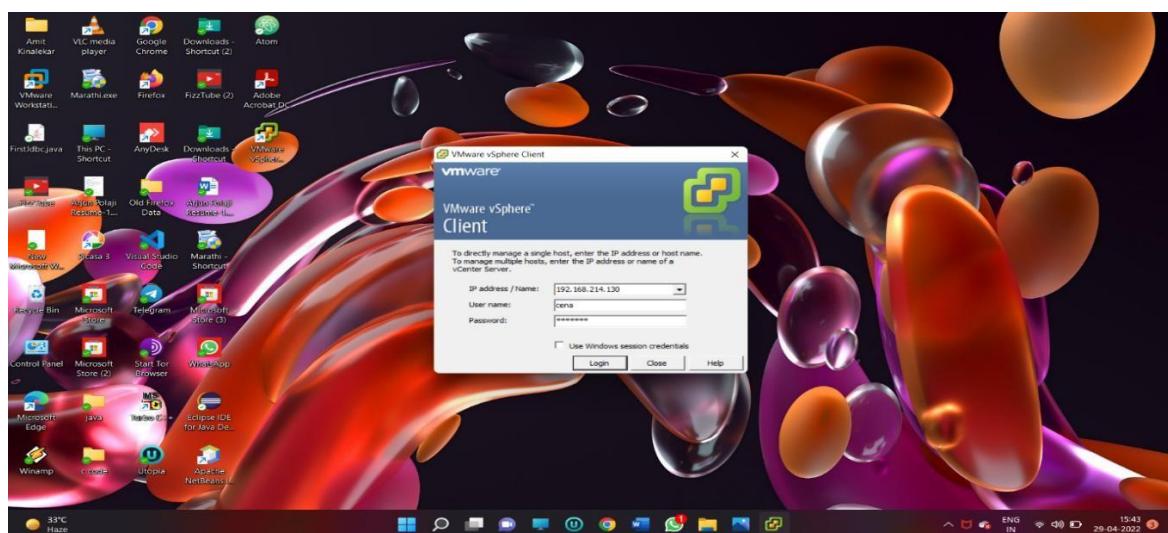
## Step 8 – Press Enter to continue



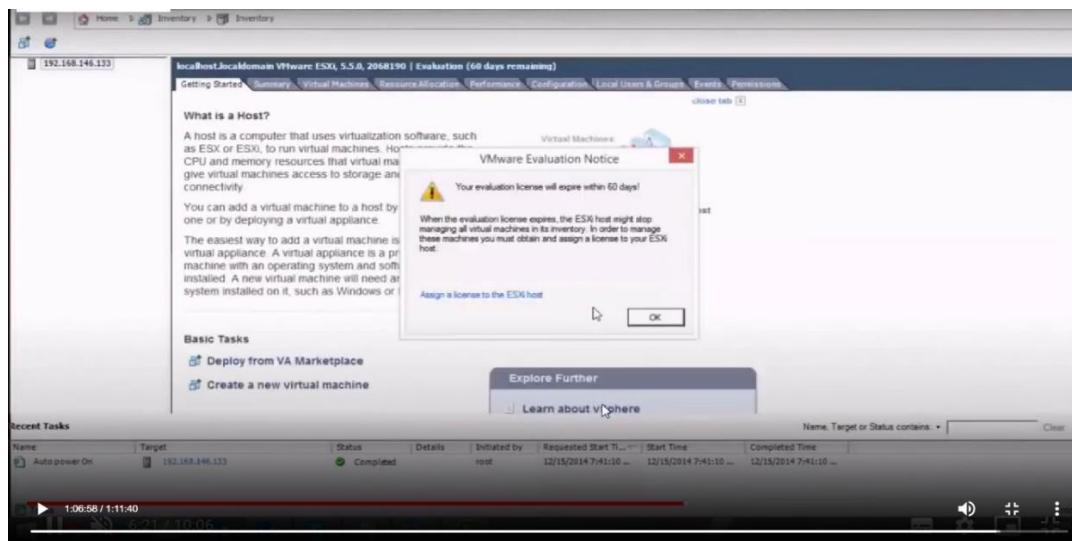
## Step 9 – Server successfully install



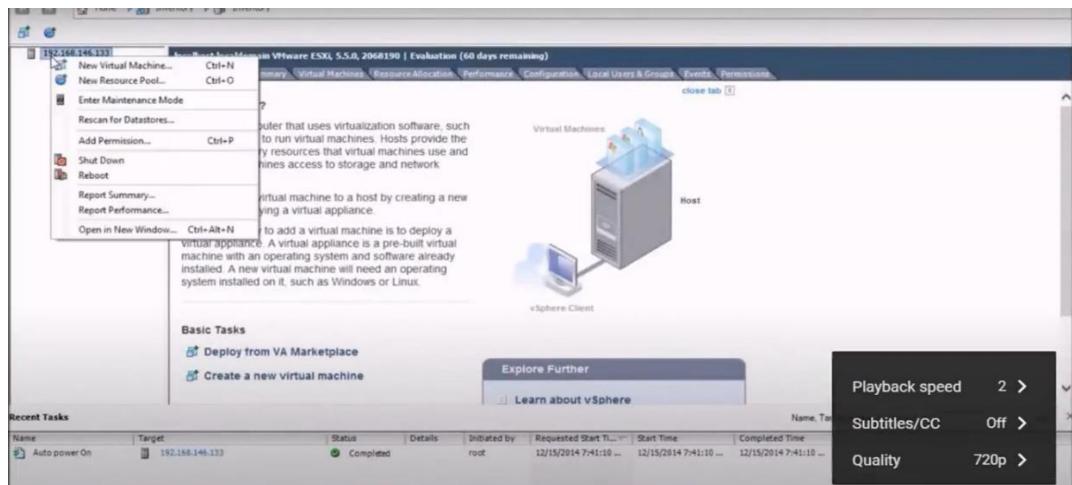
## Step 10 – Open VMware Vsphere. Client. Enter Ip address and password.



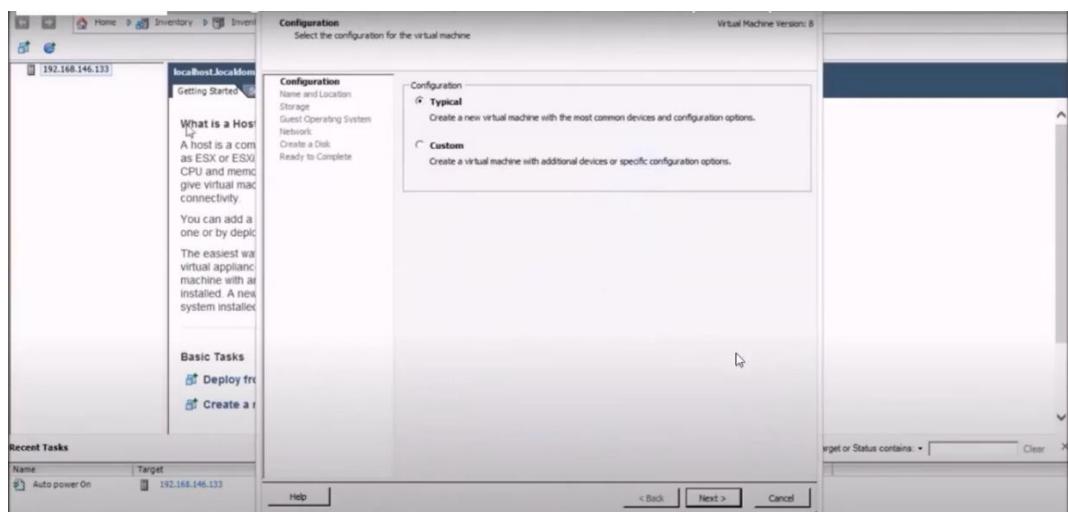
## Localhost VMware ESXI window is opened



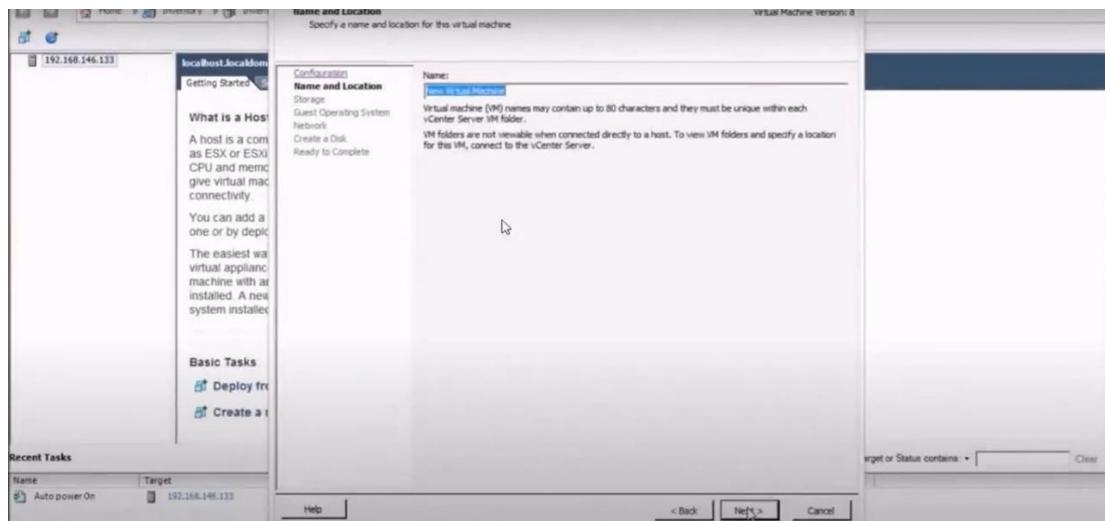
## Step 11- Click address to create virtual machine



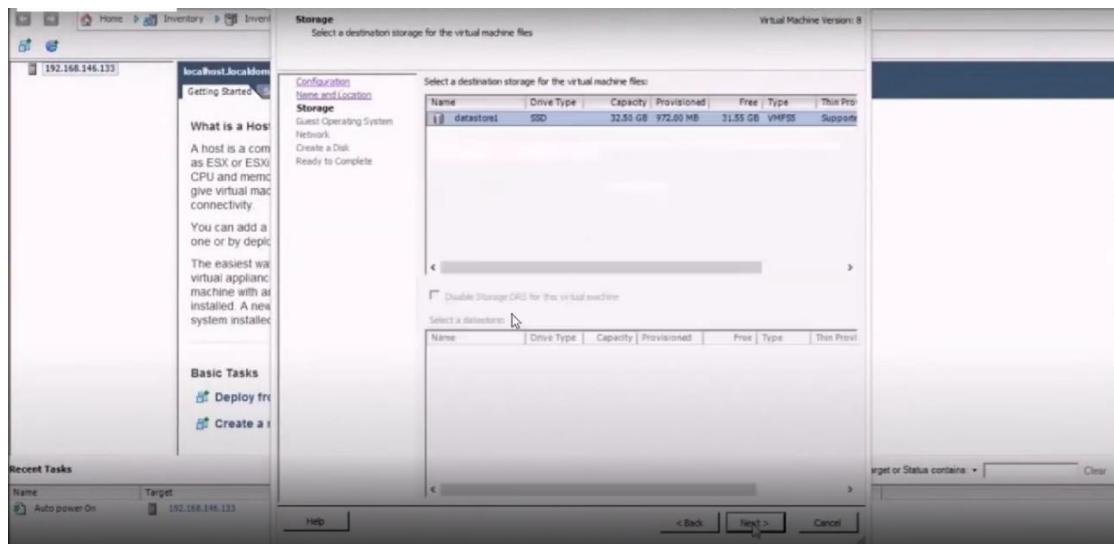
## Step 12- Select configuration for virtual machine.



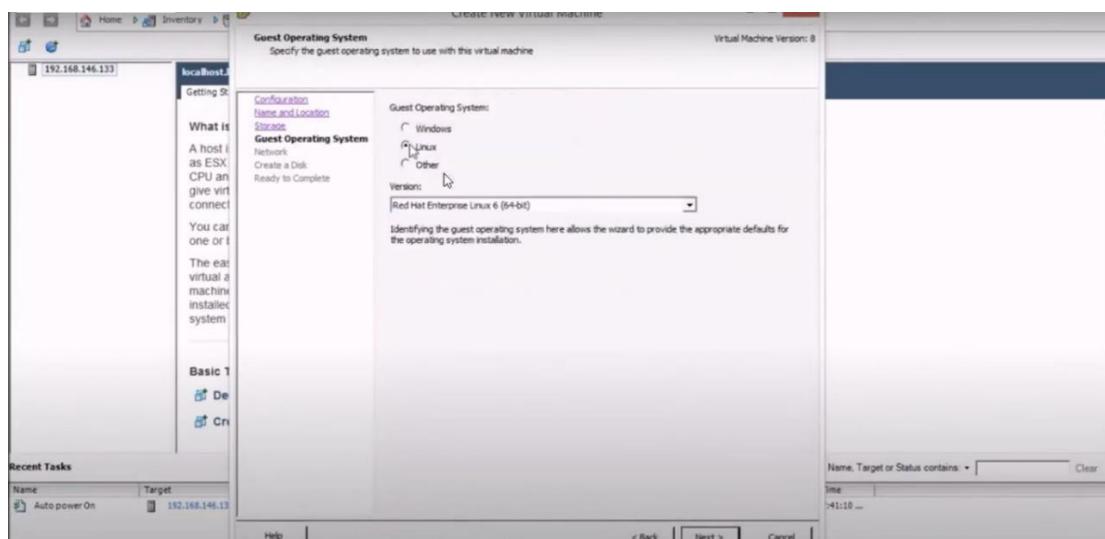
## Step 13- Specify name and location for virtual machine.



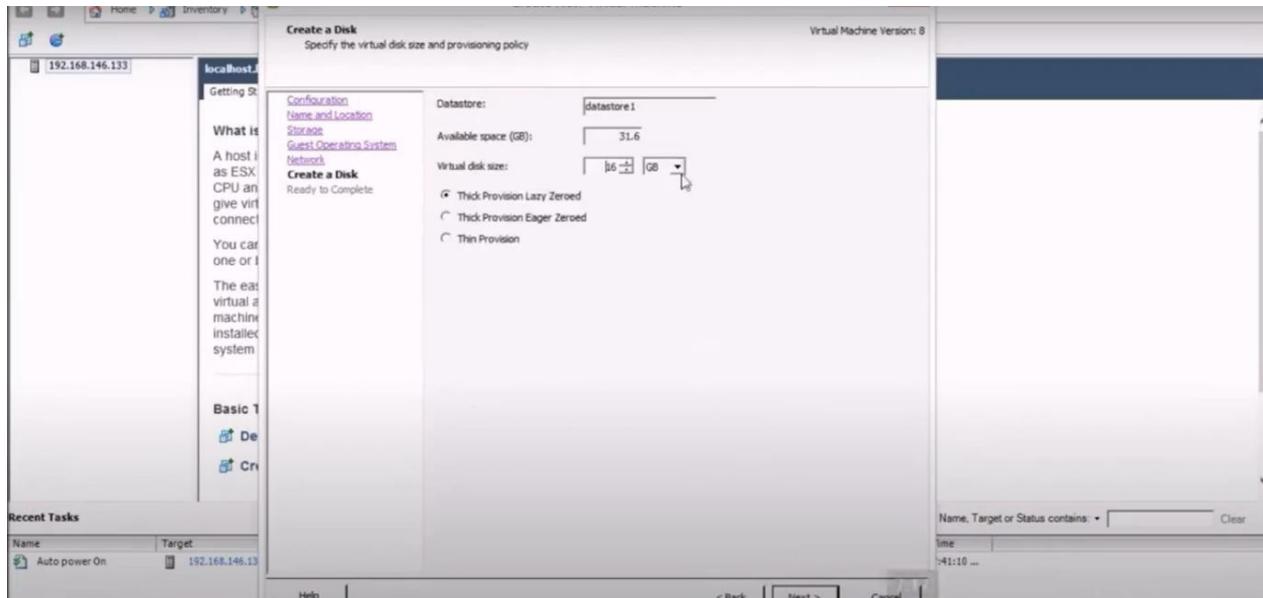
## Step 14- Select destination storage for virtual machine files.



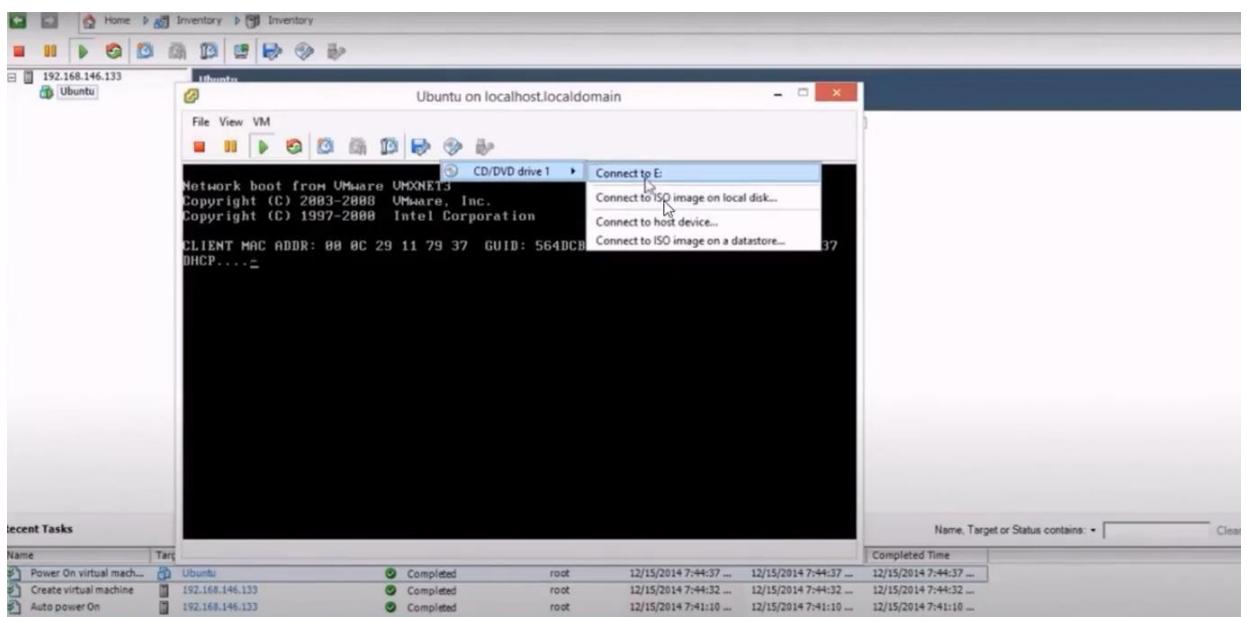
## Step 15- Select guest operating system

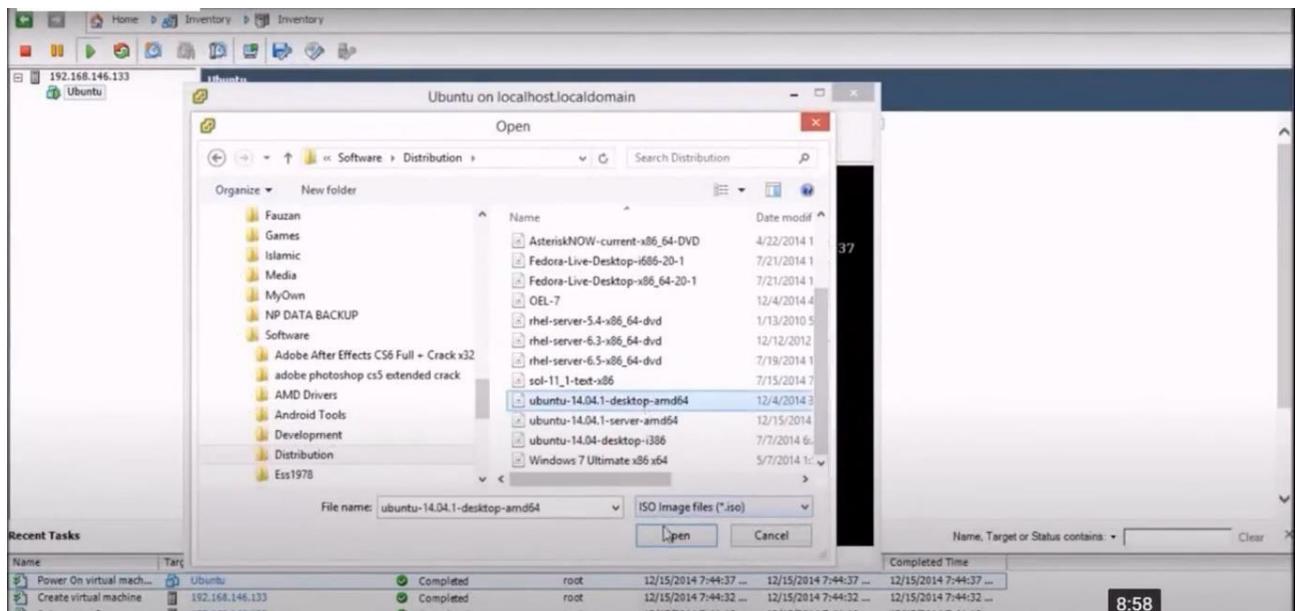


## Step 16- Specify disk size

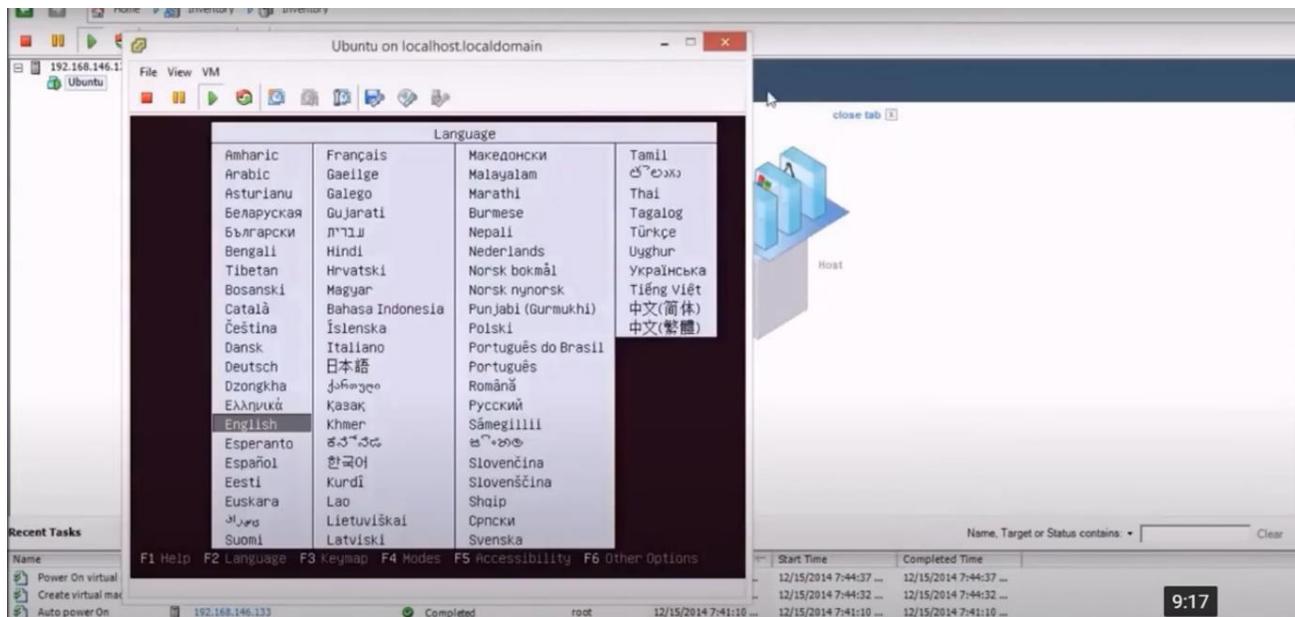


## Step 17- Select ISO file





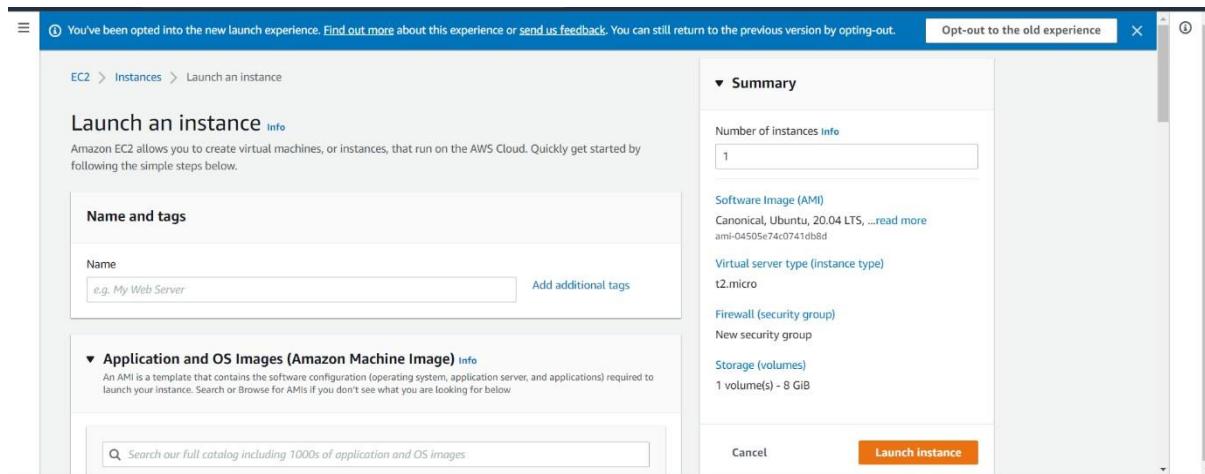
## UBUNTU SUCCESSFULLY RUNS



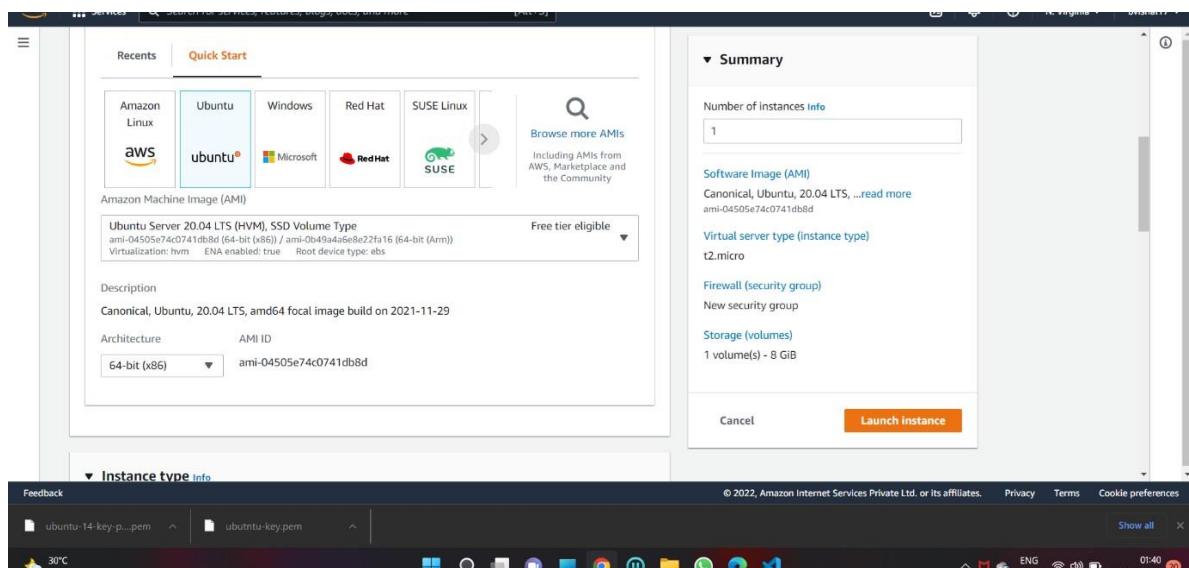
## EXPERIMENT NO.4

**Aim:** - To study and Implement Infrastructure as aService using AWS/Microsoft Azure

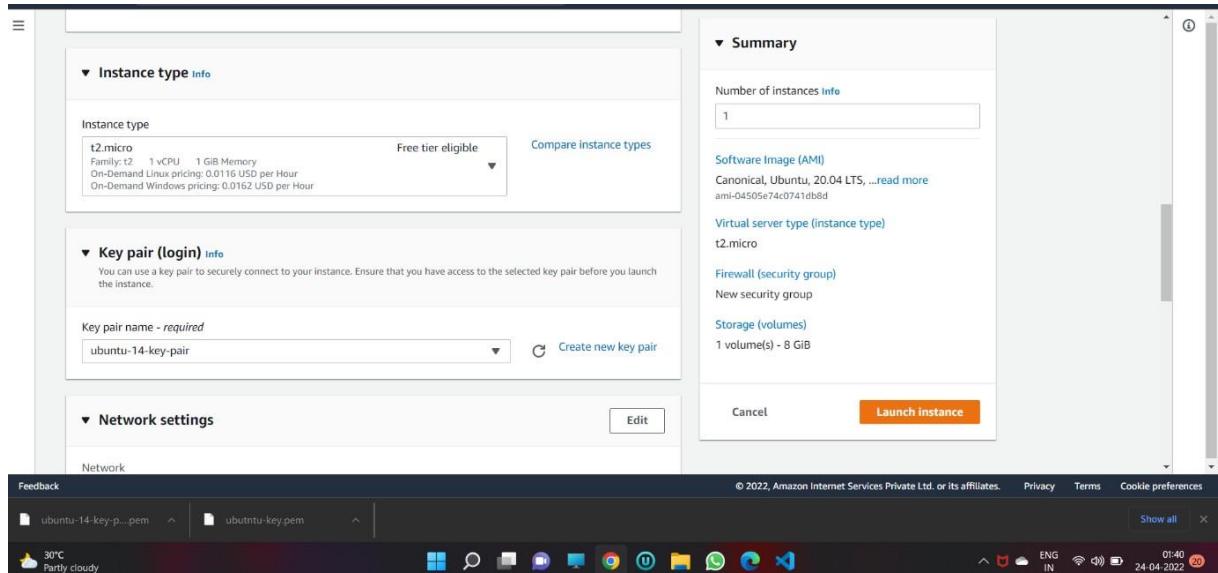
Step 1 open AWS



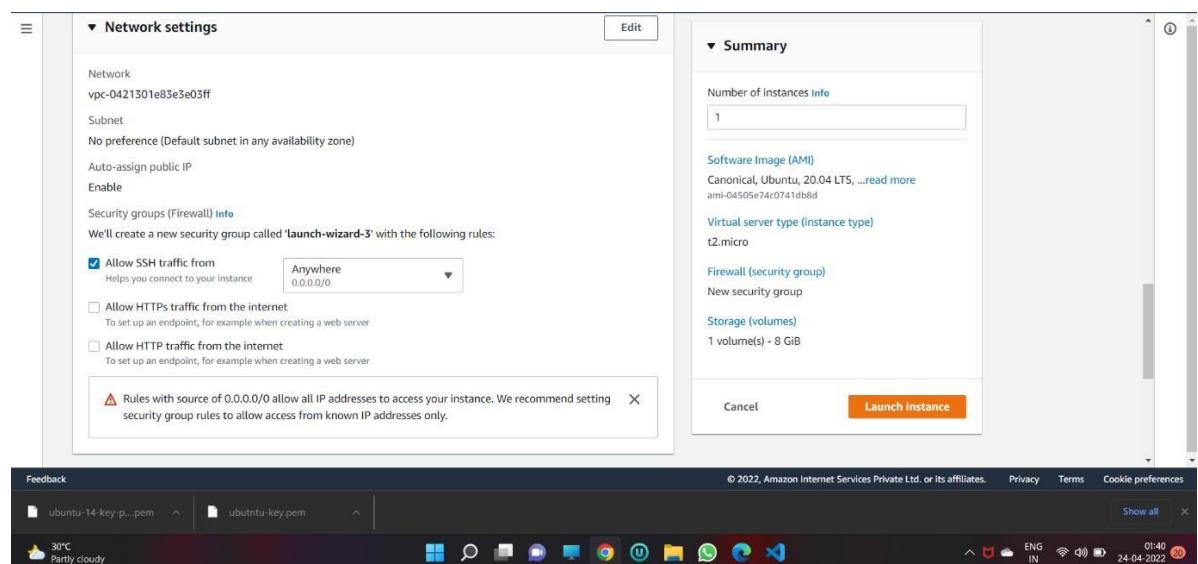
Step 2 select operating system.



### Step 3 – create new key pair



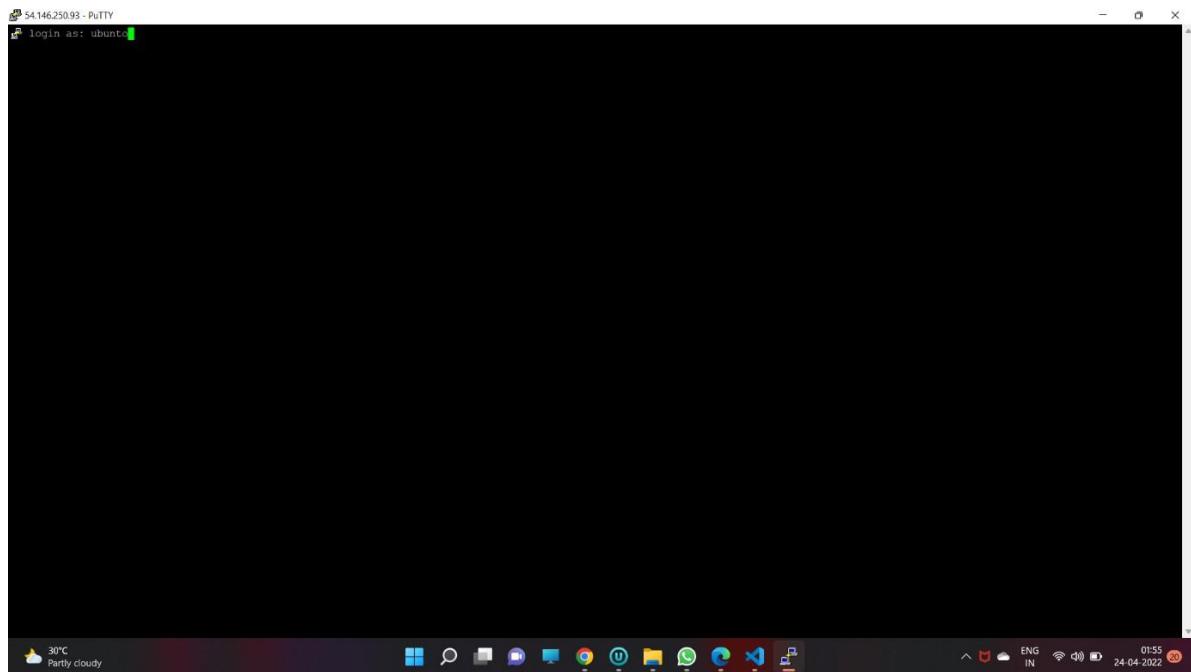
### Step 4- select allow SSH from anywhere



## Step- 5-Launch instance

The screenshot shows the AWS EC2 Instances Launch Experience page. At the top, a message says "You've been opted into the new launch experience. Find out more about this experience or send us feedback. You can still return to the previous version by opting-out." There is a "Opt-out to the old experience" button. Below this, the breadcrumb navigation shows "EC2 > Instances > Launch an instance". A success message box contains a green checkmark icon, the word "Success", and the text "Successfully initiated launch of instance (i-031bfea4d9e150b20)". A "Launch log" link is also present. A "Next Steps" section follows, containing links for "Get notified of estimated charges", "How to connect to your instance", and "View more resources to get you started". The bottom of the screen shows the Windows taskbar with various pinned icons and system status indicators.

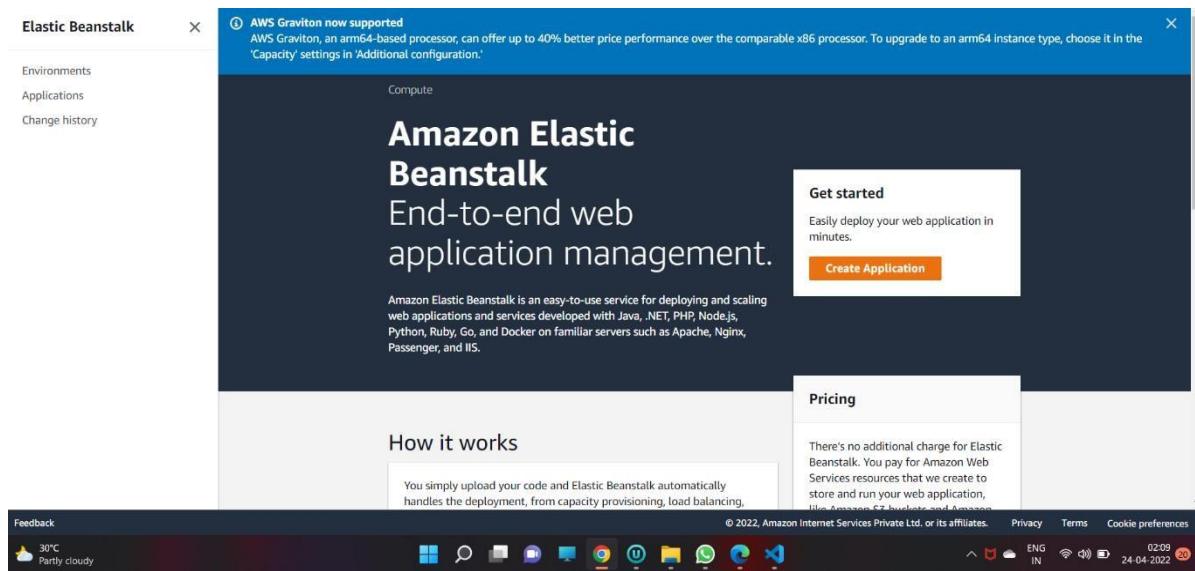
## Step -6 launce ubuntu



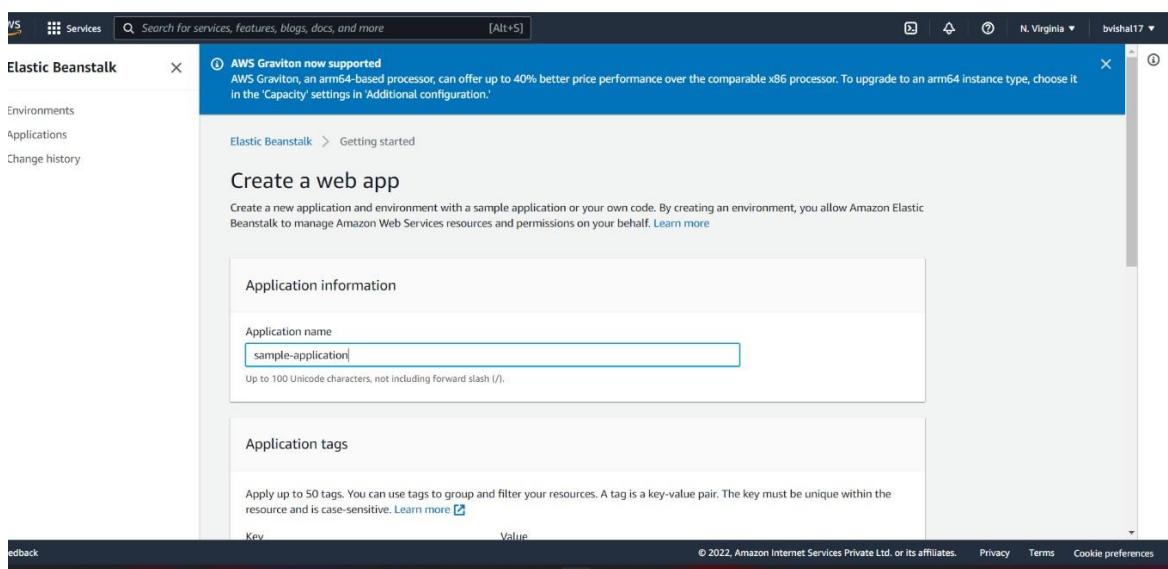
## EXPERIMENT NO.5

**Aim:** - To study and Implement Platform as a Service using AWS Elastic Beanstalk/ Microsoft Azure App Service.

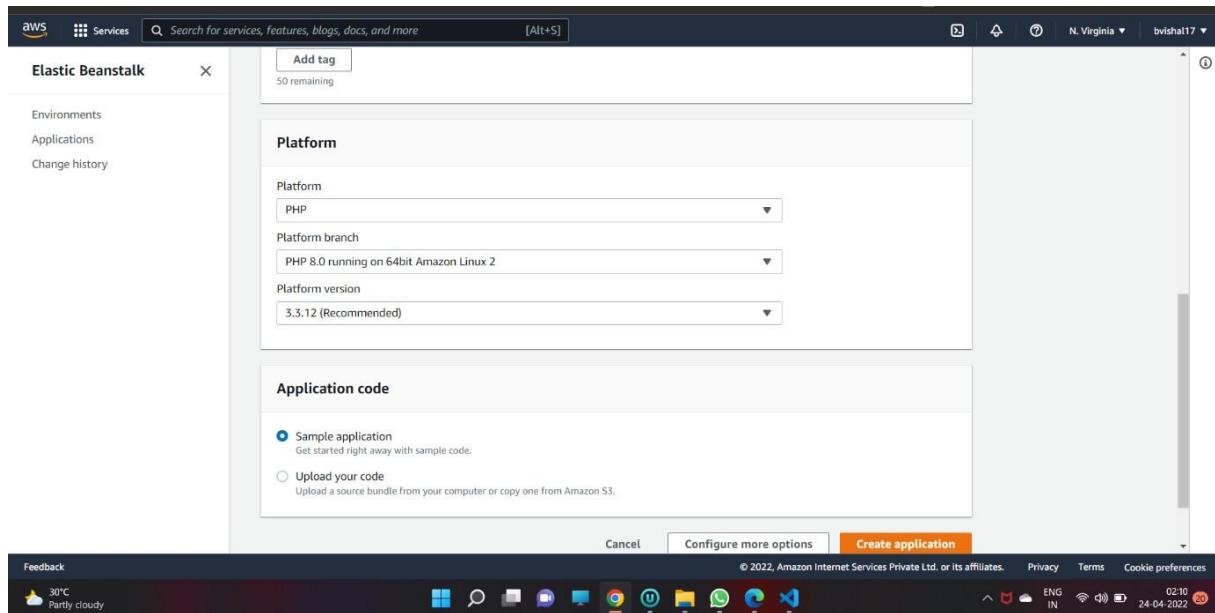
Step-1: Open AWS and select elastics beamstalk.



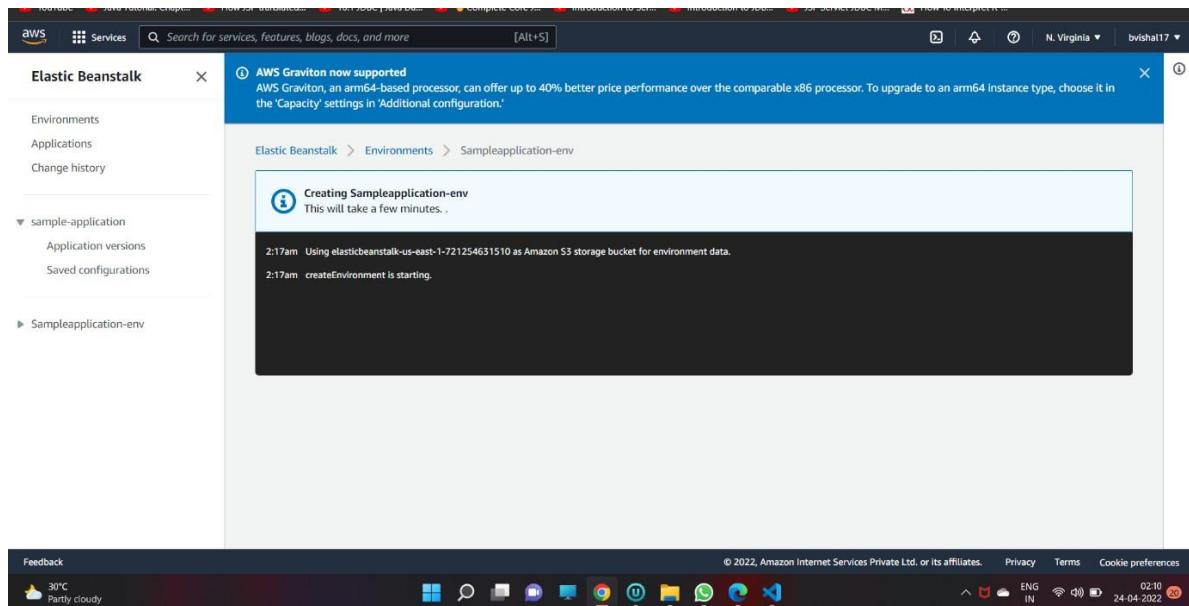
Step-2 Create web application and enter the name of application.



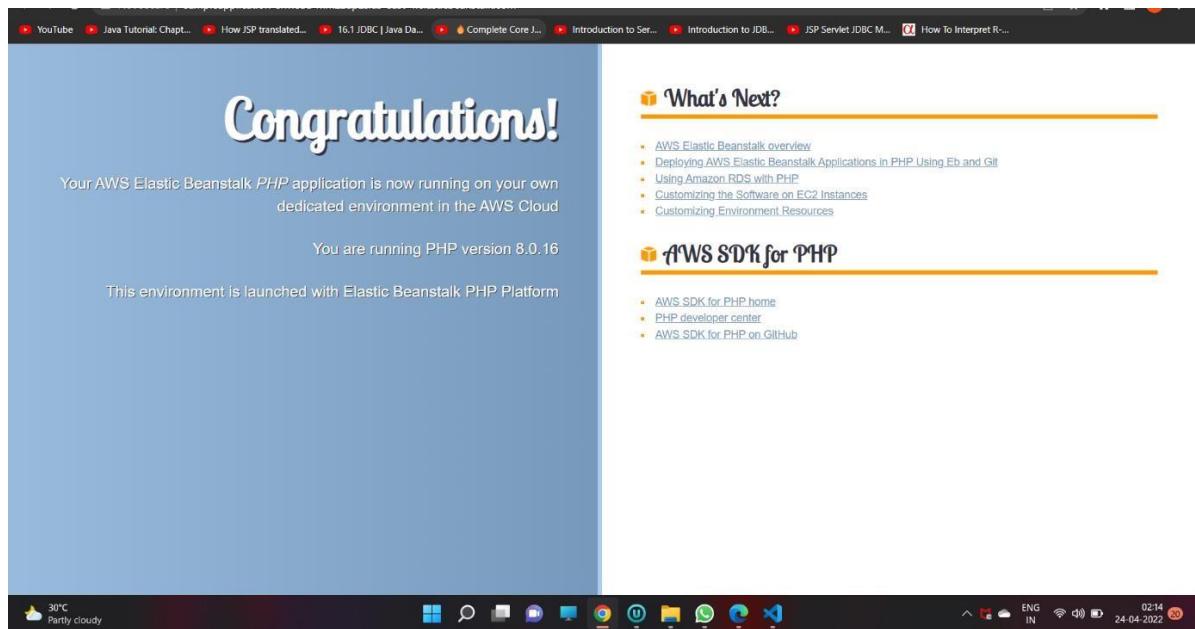
### Step-3 : Select platform and application code.



### Step 4- Click create application



Step-5 Copy link and open in the Brower.



## **EXPERIMENT NO. 6**

---

**Aim: To study and Implement Storage as a Service using Own Cloud/ AWS S3,Glaciers/Azure Storage.**

### **Theory:**

#### **Storage as a Service or SaaS**

Storage as a Service or STaaS is cloud storage that you rent from a Cloud Service Provider (CSP) and that provides basic ways to access that storage. Enterprises, small and medium businesses, home offices, and individuals can use the cloud for multimedia storage, data repositories, data backup and recovery, and disaster recovery. There are also higher-tier managed services that build on top of STaaS, such as Database as a Service, in which you can write data into tables that are hosted through CSP resources.

The key benefit to STaaS is that you are offloading the cost and effort to manage data storage infrastructure and technology to a third-party CSP. This makes it much more effective to scale up storage resources without investing in new hardware or taking on configuration costs. You can also respond to changing market conditions faster. With just a few clicks you can rent terabytes or more of storage, and you don't have to spin up new storage appliances on your own.

#### **Working of Storage as a Service :**

Some STaaS offerings can be rented based on quantity, others are rented based on a service level agreement (SLA). SLAs help establish and reinforce conditions for using data storage, such as uptime and read/write access speed. The storage you choose will typically depend on how often you intend to access the data. Cold data storage is data that you leave alone or access infrequently, whereas warm or hot data is accessed regularly and repeatedly. Pricing by quantity tends to be more cost efficient but isn't intended to support fast and frequent access for day-to-day business productivity. For hot or warm data, an SLA will be crucial to

leveraging data storage in support of current projects or ongoing processes.

Many CSPs make it easy to onboard and upload data into their STaaS infrastructure for little to no cost at all. However, there may be hidden fees and it can be extremely costly to migrate or transfer your data to a different cloud platform.

The screenshot shows the AWS Management Console homepage. At the top, there's a navigation bar with the AWS logo, a 'Services' dropdown, a 'Resource Groups' dropdown, a user icon, and a 'Support' link. Below the navigation is a search bar and a 'Region' dropdown set to 'N. Virginia'. The main content area has a title 'AWS Management Console' and a 'AWS services' section. In the 'Find Services' search bar, the text 'S3' is typed. A list of services begins with 'S3 Storage in the Cloud' (highlighted in light blue), followed by 'S3 Glacier', 'AWS Transfer for SFTP', 'Athena', 'Snowball', 'Amazon Transcribe', 'ECR', 'ECS', 'EKS', 'Lambda', 'Batch', 'Elastic Beanstalk', and 'Storage'. To the right of the service list are two boxes: 'Access resources on the go' (with a mobile phone icon) and 'Explore AWS' (with sections for 'Amazon Redshift', 'Amazon RDS', and 'Run Serverless Containers with AWS Fargate').

The screenshot shows the AWS S3 Management Console interface. On the left, there's a sidebar with 'Amazon S3' and 'Buckets'. The main area is titled 'S3 buckets' and displays a single bucket entry:

Bucket name	Access	Region	Date created
elasticbeanstalk-us-east-1-553775641836	Objects can be public	US East (N. Virginia)	Feb 1, 2019 10:12:02 PM GMT+0530

Below the table, there are buttons for 'Create bucket', 'Edit public access settings', 'Empty', and 'Delete'. At the bottom, there are tabs for 'Operations' (0 In progress, 0 Success, 2 Error), 'Feedback', 'English (US)', and links to 'Privacy Policy' and 'Terms of Use'.

The screenshot shows the 'Create bucket' wizard, step 1: Name and region. The page has tabs at the top: 1. Name and region, 2. Configure options, 3. Set permissions, 4. Review. The 'Name and region' section contains:

- Bucket name:** loc
- Regions:** US East (N. Virginia)
- Copy settings from an existing bucket:** Saved bucket (plutovalt1 Buckets)

At the bottom are 'Create' and 'Cancel' buttons, and a 'Next Step' link.

S3 Management Console https://console.aws.amazon.com/s3/home?region=us-east-1

BWS Services Resource Groups Support

Create bucket

① Name and region ② Configure options ③ Set permissions ④ Review

**Properties**

**Versioning**  
 Keep all versions of an object in the same bucket. [Learn more](#)

**Server access logging**  
 Log requests for access to your bucket. [Learn more](#)

**Tags**  
You can use tags to track project costs. [Learn more](#)

Key Value [Add another](#)

**Object level logging**  
 Record object-level API activity using AWS CloudTrail for an additional cost. See [CloudTrail pricing](#) or [Learn more](#)

**Default encryption**  
 Automatically encrypt objects when they are stored in S3. [Learn more](#)

+ Advanced settings

Previous Next

Feedback English (US) © 2018 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

S3 Management Console https://console.aws.amazon.com/s3/home?region=us-east-1

BWS Services Resource Groups Support

Create bucket

① Name and region ② Configure options ③ Set permissions ④ Review

**Public access settings for this bucket**

Use the Amazon S3 block public access settings to enforce that buckets don't allow public access to data. You can also configure the Amazon S3 block public access settings at the account level. [Learn more](#)

Manage public access control lists (ACLs) for this bucket [?](#)

Block new public ACLs and uploading public objects (Recommended) [?](#)

Remove public access granted through public ACLs (Recommended) [?](#)

Manage public bucket policies for this bucket [?](#)

Block new public bucket policies (Recommended) [?](#)

Block public and cross-account access if bucket has public policies (Recommended) [?](#)

Manage system permissions

Do not grant Amazon S3 Log Delivery group write access to this bucket

Previous Next

Feedback English (US) © 2018 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

S3 Management Console https://console.aws.amazon.com/s3/home?region=us-east-1

Services Resource Groups Global Support

### Create bucket

Name and region  Configure options  Set permissions  Review

Name and region

Bucket name: **lcoe** Region: US East (N. Virginia)

Options

Versioning	Disabled
Server access logging	Disabled
Tagging	0 Tags
Object-level logging	Disabled
Default encryption	None
CloudWatch request metrics	Disabled
Object lock	Disabled

Permissions

Block new public ACLs and uploading public objects	True
Remove public access granted through public ACLs	True

[Previous](#) [Create bucket](#)

Feedback English (US) © 2025 - 2018 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

S3 Management Console https://console.aws.amazon.com/s3/buckets/lcoe?region=us-east-1&tab=review

Services Resource Groups Global Support

Amazon S3 > lcoe

Overview Properties Permissions Management

Upload Create folder Download Actions US East (N. Virginia)

This bucket is empty. Upload new objects to get started.

**Upload an object** **Set object properties** **Set object permissions**

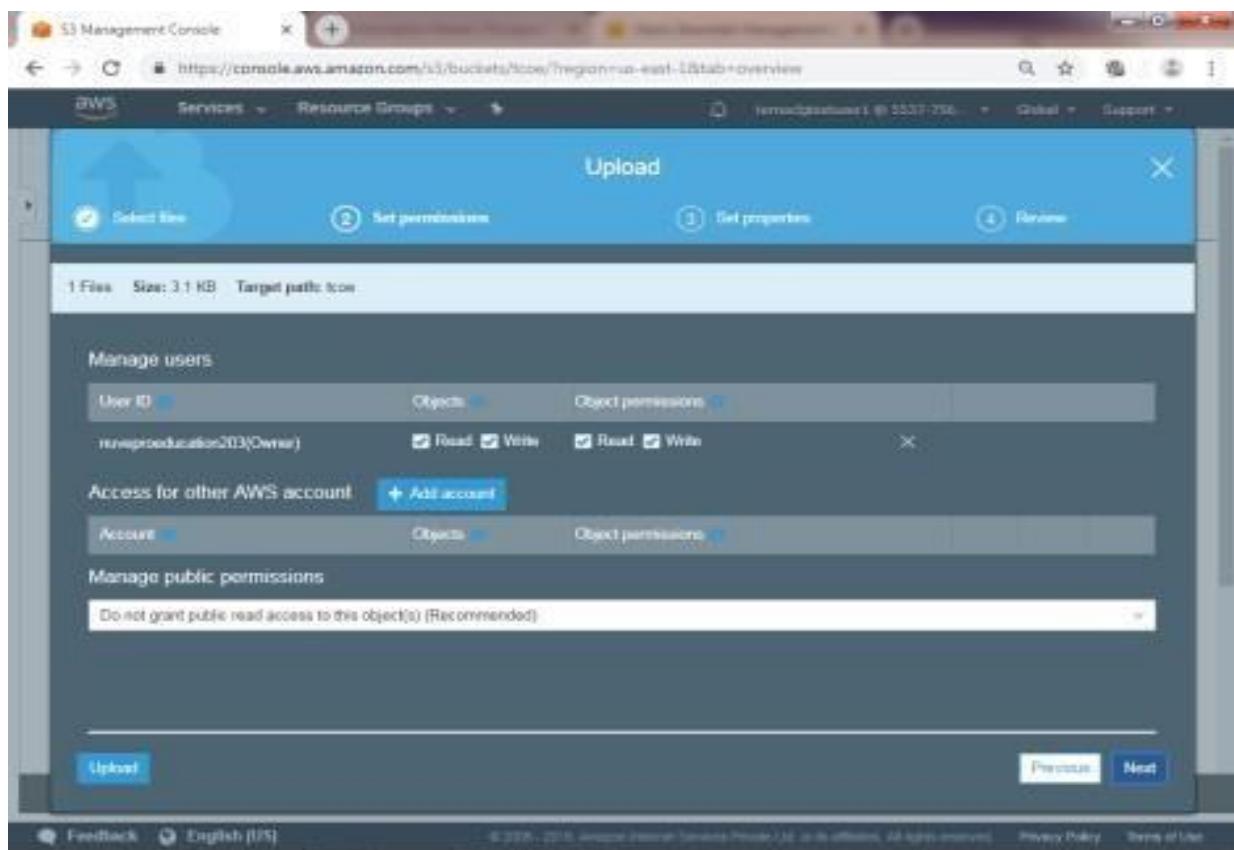
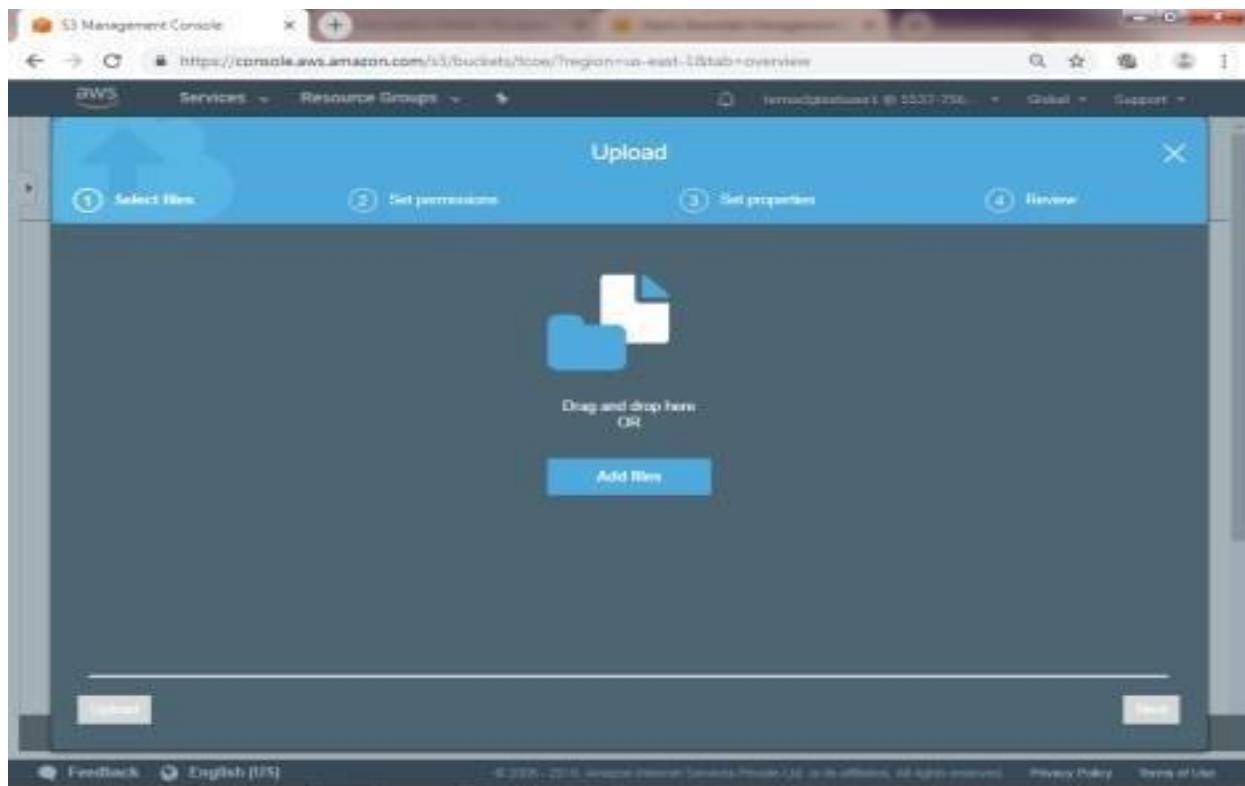
Buckets are globally unique containers for everything that you store in Amazon S3.

After you create a bucket, you can upload your objects. (For example, your photo or video files.)

By default, the permissions on an object are private, but you can set up access control policies to grant permissions to others.

Operations 0 In progress 0 Success 2 Error

Feedback English (US) © 2025 - 2018 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use



S3 Management Console New Feature Overview

https://console.aws.amazon.com/s3/buckets/testregionus-east-1/test+overview

Services Resource Groups Global Support

### Upload

1 File Size: 3.1 KB Target prefix: icon

Storage class

Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
Standard	Frequently accessed data	≥ 3	-	-	-	-
Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-	Per-object fees apply	-
Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per-GB fees apply
One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per-GB fees apply
Glacier	Data archiving with retrieval times ranging from minutes to hours	≥ 3	90 days	-	-	Per-GB fees apply
Reduced Redundancy	Frequently accessed, non-critical	≥ 3	-	-	-	-

**Upload** Previous Next

Feedback English (US) © 2016 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

S3 Management Console New Feature Overview

https://console.aws.amazon.com/s3/buckets/testregionus-east-1/test+overview

Services Resource Groups Global Support

### Upload

1 File Size: 3.1 KB

Files

Permissions

Properties

Encryption No Storage class Standard

Metadata

Tag

Edit Previous Upload

Feedback English (US) © 2016 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

S3 Management Console

https://console.aws.amazon.com/s3/buckets/tsecwebapp?region=us-east-1&tab=overview

aws Services Resource Groups

Amazon S3 > tsecwebapp

Overview Properties Permissions Management

Type a prefix and press Enter to search. Press ESC to clear.

Upload Create folder Download Actions US East (N. Virginia) Viewing 1 to 1

Name	Last modified	Size	Storage class
tsecwebapp-1.0-SNAPSHOT.war	Feb 1, 2019 11:35:18 PM GMT+0530	3.1 KB	Standard

Viewing 1 to 1

Operations 0 In progress 1 Success 2 Error

Feedback English (US) © 2006 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

S3 Management Console

https://console.aws.amazon.com/s3/object/tsecwebapp-1.0-SNAPSHOT.war?region=us-east-1&tab=properties

aws Services Resource Groups

Amazon S3 > tsecwebapp > tsecwebapp-1.0-SNAPSHOT.war

tsecwebapp-1.0-SNAPSHOT.war Latest version +

Overview Properties Permissions Select type

Open Download Download as Make public Copy path

**Owner**  
naveenreddy203

**Last modified**  
Feb 1, 2019 11:35:18 PM GMT+0530

**Etag**  
S05803353563462e2f0a26702987fbd

**Storage class**  
Standard

**Server-side encryption**  
None

**Size**  
3.1 KB

**Key**  
tsecwebapp-1.0-SNAPSHOT.war

**Object URL**  
<https://s3.amazonaws.com/tsecwebapp/tsecwebapp-1.0-SNAPSHOT.war>

https://s3.amazonaws.com/tsecwebapp/tsecwebapp-1.0-SNAPSHOT.war © 2006 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

B) S3  
Glacier  
S

The screenshot shows the AWS S3 Management Console interface. The left sidebar has 'Amazon S3' selected, with 'Buckets' and 'Public access settings for this account' also visible. The main content area is titled 'Public access settings for this account' and includes a note about using Amazon S3 block public access settings to enforce that buckets don't allow public access to data. It lists two sections: 'Manage public access control lists (ACLs)' and 'Manage public bucket policies'. Both sections show 'False' under 'Block new public [setting]' and 'False' under '[setting] (Recommended)'. At the bottom, there are links for 'Feedback', 'English (US)', and copyright information.

Public access settings for this account

Use the Amazon S3 block public access settings to enforce that buckets don't allow public access to data. You can also configure the Amazon S3 block public access settings at the bucket level. [Learn more](#)

Manage public access control lists (ACLs)	Manage public bucket policies
Block new public ACLs and uploading public objects (Recommended) False	Block new public bucket policies (Recommended) False
Remove public access granted through public ACLs (Recommended) False	Block public and cross-account access to buckets that have public policies (Recommended) False

Feedback English (US) © 2006 - 2019, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use Show all X

The screenshot shows the AWS Management Console home page. At the top, there is a navigation bar with links for 'Services', 'Resource Groups', and 'Support'. The main title 'AWS Management Console' is centered above a search bar and a 'Find Services' input field containing 's3 glacier'. Below this, there are two main sections: 'AWS services' and 'Access resources on the go'.

**AWS services**

- Find Services:** You can enter names, keywords or acronyms.  
s3 glacier
- S3 Glacier**: Archive Storage in the Cloud
- Snowball**: Large Scale Data Transfers
- Elastic Beanstalk**
- EC2**
- IAM**

**All services**

- Compute**
  - EC2
  - Lightsail
  - ECR
  - ECS
  - EKS
  - Lambda
  - Batch
  - Elastic Beanstalk
- Machine Learning**
  - Amazon SageMaker
  - Amazon Comprehend
  - AWS DeepLens
  - Amazon Lex
  - Machine Learning
  - Amazon Polly
  - Rekognition
  - Amazon Transcribe

**Access resources on the go**

Access the Management Console using the AWS Console Mobile App. Learn more [\[link\]](#)

**Explore AWS**

**Amazon SageMaker**  
Build, train, and deploy machine learning models. [Learn more \[link\]](#)

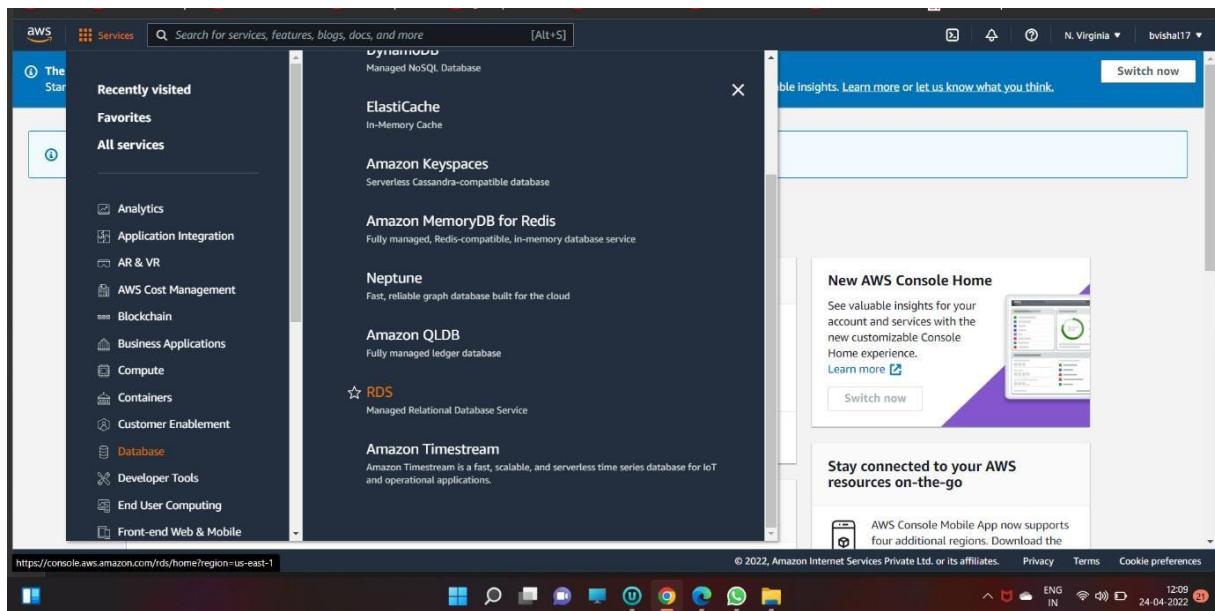
**Run Serverless Containers with AWS Fargate**  
AWS Fargate runs and scales your containers without having to manage servers or clusters. [Learn more \[link\]](#)

**AWS Marketplace**  
Find, buy, and deploy popular software products that run on AWS. [Learn more \[link\]](#)

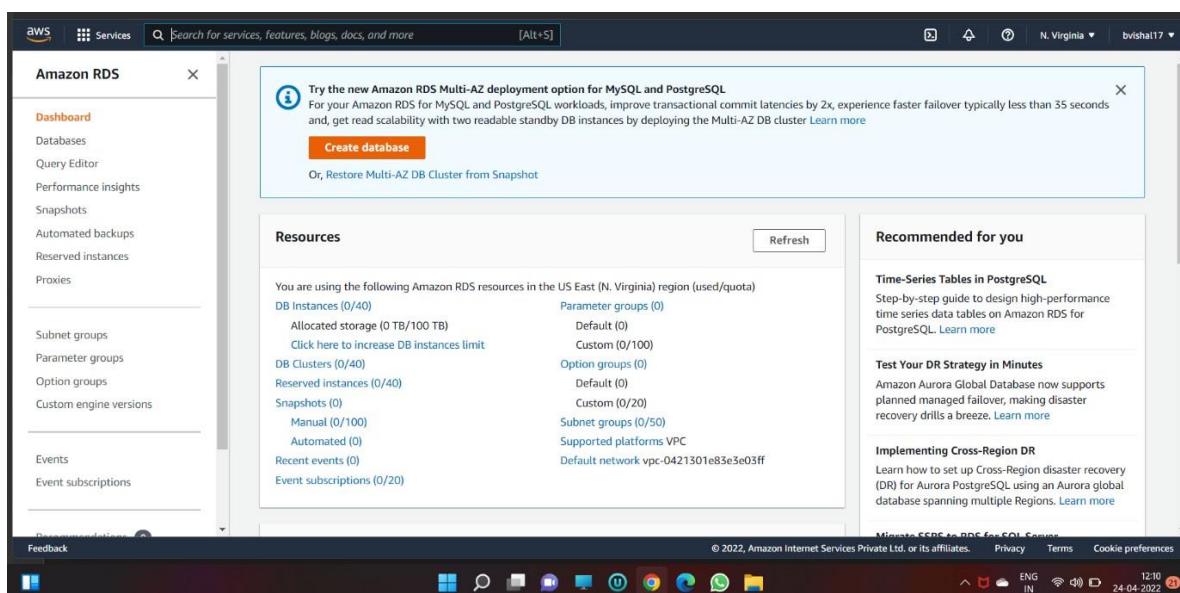
## EXPERIMENT NO.7

**Aim:** - To study and Implement Database as a Service onSQL/NOSQL databases like AWS RDS, AZURE SQL/ MongoDB Lab/ Firebase.

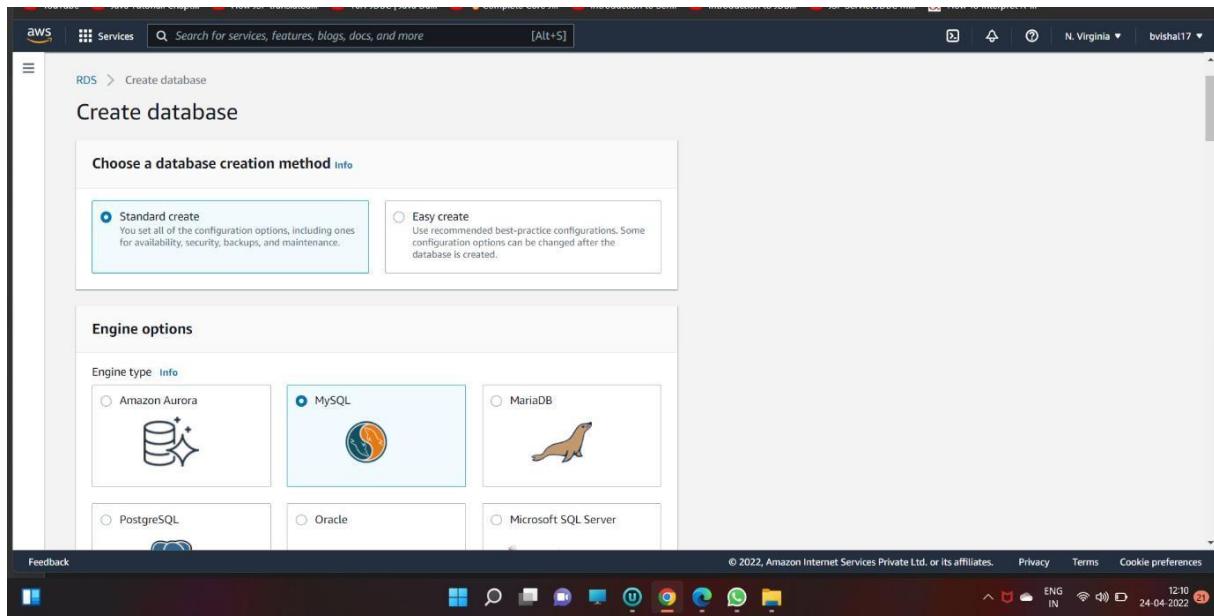
Step- 1: Open AWS and open RDS service



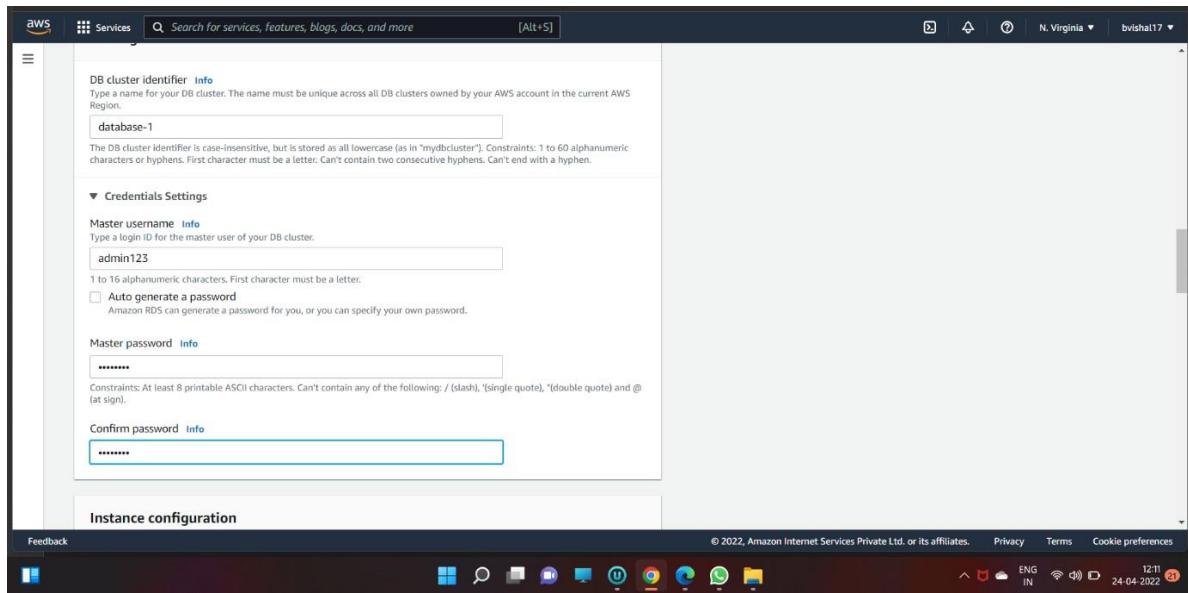
Step 2 : Click on create database



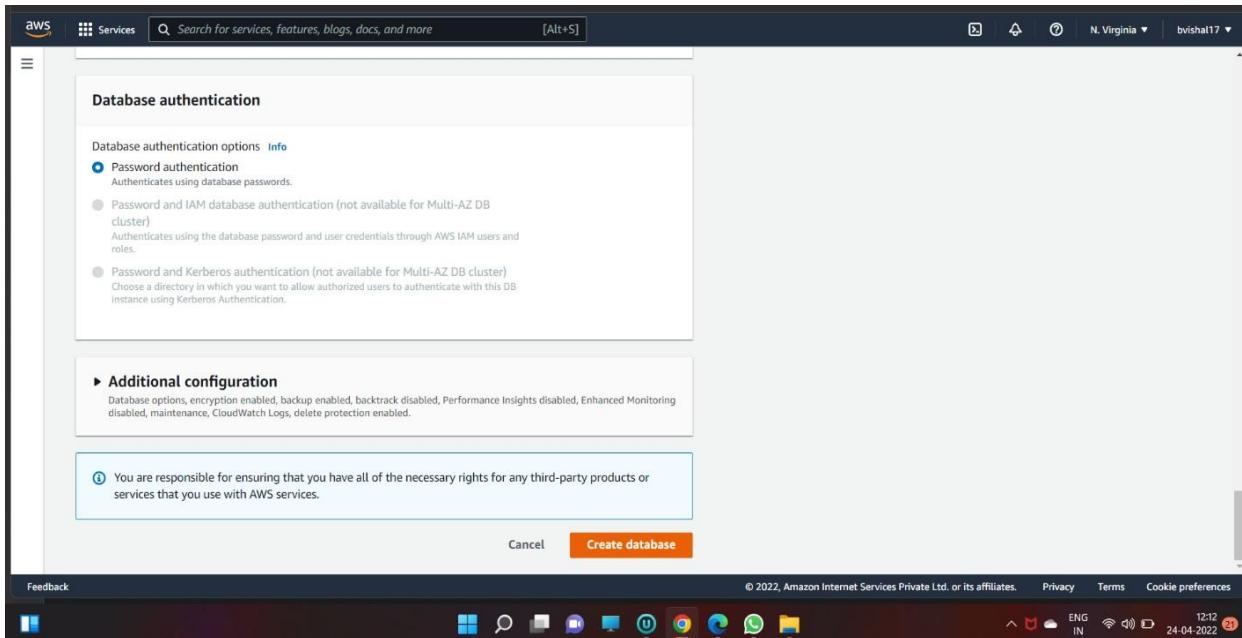
### Step 3 select engine option as mysql



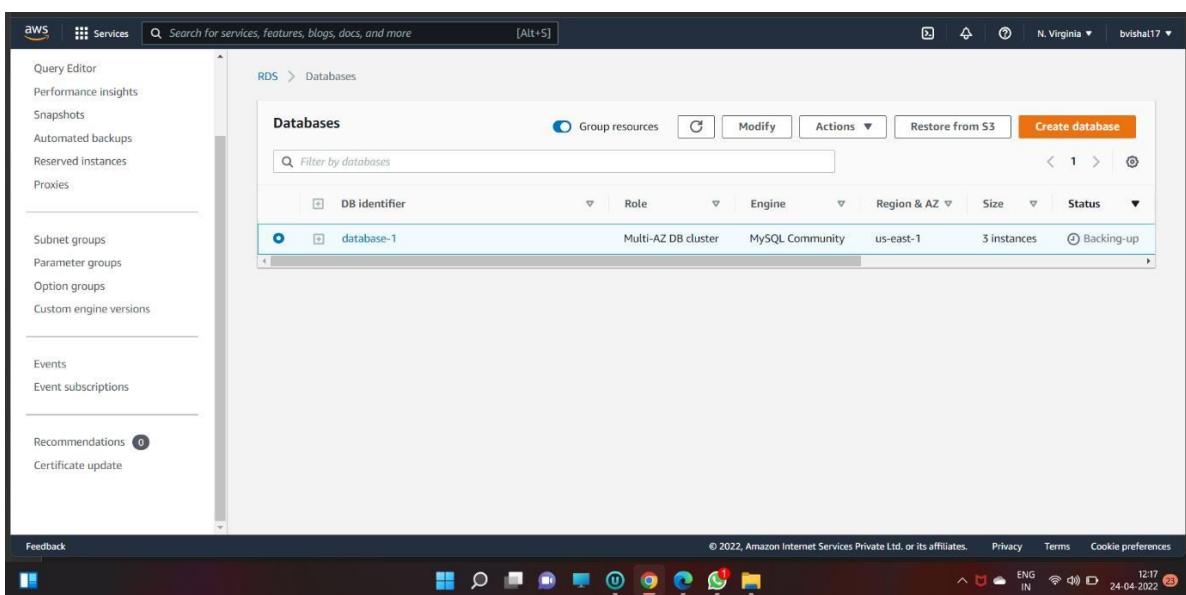
### Step 4 : Create username and password



## Step 5: Click on create database



Database created



## EXPERIMENT NO 8

**AIM:** To study and Implement Security as a Service on AWS/Azure

**STEP 1:** Open the AWS home page, Search the IAM, Open the IAM dashboard,

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar menu includes 'Identity and Access Management (IAM)' (selected), 'Dashboard', 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings), 'Access reports' (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)), and 'AWS Account' (Account ID, Account Alias, Sign-in URL, Create). The main content area has a banner 'Introducing the new IAM dashboard experience' with a link to 'Let us know what you think'. It features 'Security recommendations' with a red warning icon for 'Add MFA for root user' and a green checkmark for 'Root user has no active access keys'. Below is the 'IAM resources' section with counts: User groups (0), Users (0), Roles (7), Policies (0), and Identity providers (0). A 'What's new' section lists recent changes like 'Right-size permissions for more roles' and 'Amazon S3 Object Ownership'. On the right, there are 'Quick Links' (My security credentials, Manage your access keys, multi-factor authentication (MFA) and other credentials) and 'Tools' (Policy simulator). The bottom navigation bar includes links for 'Web identity federation playground', '© 2022, Amazon Internet Services Private Ltd. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

**STEP 2:** Create one user group: **MITM\_TE**

The screenshot shows the 'Create user group' wizard in the AWS IAM console. The sidebar is identical to the previous screenshot. The main steps are: 'Name the group' (User group name: MITM\_TE), 'Add users to the group - Optional (0) (Info)', and 'Attach permissions policies - Optional (750) (Info)'. The 'Add users to the group' step shows a search bar and a table with columns: User name, Groups, Last activity, and Creation time. The table is empty with the message 'No resources to display'. The 'Attach permissions policies' step shows a note: 'You can attach up to 10 policies to this user group. All the users in this group will have' and a 'Create Policy' button. The bottom navigation bar includes links for 'Feedback', '© 2022, Amazon Internet Services Private Ltd. or its affiliates.', 'Privacy', 'Terms', and 'Cookie preferences'.

STEP 3: MITM TE group created. NO user is present in this group.

The screenshot shows the AWS IAM User Groups page. A green banner at the top indicates that the 'MITM\_TE' user group has been created. The main table lists two groups: 'MITM-COMPUTER' and 'MITM\_TE'. Both groups have 3 users and 'Not defined' permissions. The 'Creation time' for both is 'Now'.

Group name	Users	Permissions	Creation time
MITM-COMPUTER	3	Not defined	12 minutes ago
MITM_TE	0	Not defined	Now

#### Step 4: Add USER in MITM\_TE group

The screenshot shows the 'Set user details' step of the 'Add user' wizard. The user name is set to 'mitm\_user'. The 'Select AWS access type' section shows that 'Access key - Programmatic access' is selected, which enables programmatic access via an access key ID and secret access key. The next step, 'Next: Permissions', is visible at the bottom.

The screenshot shows the 'Add user to group' step of the 'Add user' wizard. It shows the 'Add user to group' interface with a search bar and a list of groups. 'MITM\_TE' is selected, and its attached policies are listed as 'None'. The next step, 'Next: Tags', is visible at the bottom.

AWS Services Search for services, features, blogs, docs, and more [Alt+S] Global bvishal17

### Add user

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	mitm_user
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	MITM_TE

Tags

No tags were added.

Cancel Previous Create user

AWS Services Search for services, features, blogs, docs, and more [Alt+S] Global bvishal17

### Add user

Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://721254631510.signin.aws.amazon.com/console>

[Download .csv](#)

User	Access key ID	Secret access key
mitm_user	AKIA2P3RAJBLMABRB6UT	***** Show

Close

Feedback © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search for services, features, blogs, docs, and more [Alt+S] Global bvishal17

Identity and Access Management (IAM)

Introducing the new Users list experience We've redesigned the Users list experience to make it easier to use. [Let us know what you think.](#)

IAM > Users

Users (4) Info An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

[Find users by username or access key](#)

User name	Groups	Last activity	MFA	Password age	Active key age
Amit	MITM-COMPUTER	Never	None	None	20 minutes ago
Hemant	MITM-COMPUTER	Never	None	None	20 minutes ago
mitm_user	MITM_TE	Never	None	None	1 minute ago
Vishal	MITM-COMPUTER	Never	None	None	20 minutes ago

Feedback © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

## STEP 5: Set the permission boundary to the USER , select any policy for USER

STEP 6: Assigned MFA Device, click on Manage and select the Virtual MFA Device

The screenshot shows the 'Manage MFA device' dialog box over a user summary page. The 'Virtual MFA device' option is selected. A note at the bottom states: 'For more information about supported MFA devices, see AWS Multi-Factor Authentication'. Buttons at the bottom are 'Cancel' and 'Continue'.

STEP 7: Download the Google Authenticator application on your mobile device , scan the Qr code &submit the Mfa code1 & MFA code 2.

The screenshot shows the 'Set up virtual MFA device' dialog box. Step 2 displays a QR code with the instruction 'Use your virtual MFA app and your device's camera to scan the QR code'. Step 3 shows input fields for 'MFA code 1' (008666) and 'MFA code 2' (099288). Buttons at the bottom are 'Cancel', 'Previous', and 'Assign MFA'.

AWS Services Search for services, features, blogs, docs, and more [Alt+5] Global bvbd1a17 ▾

**Identity and Access Management (IAM)**

- Dashboard
- Access management
  - User groups
  - Users**
  - Roles
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Q Search IAM AWS account ID: 721254631510 Feedback

New feature to generate a policy based on CloudTrail events. AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.

Users > mtm\_user

### Summary

User ARN am:aws:iam:721254631510:user/mtm\_user Path / Creation time 2022-04-24 13:03 UTC+0530

Permissions Groups (1) Tags Security credentials Access Advisor

**Sign-in credentials**

Summary	• User does not have console management access • MFA is required when signing in. Learn more
Console password	Disabled   Manage
Assigned MFA device	am:aws:iam:721254631510:mfa/mtm_user (Virtual)   Manage
Signing certificates	None ↗

**Access keys**

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. Learn more

Create access key

Access key ID	Created	Last used	Status
---------------	---------	-----------	--------

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

AWS Services Search for services, features, blogs, docs, and more [Alt+5] Global bvbd1a17 ▾

**Identity and Access Management (IAM)**

- Dashboard
- Access management
  - User groups
  - Users**
  - Roles
  - Policies
  - Identity providers
  - Account settings
- Access reports
  - Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Q Search IAM AWS account ID: 721254631510 Feedback

New feature to generate a policy based on CloudTrail events. AWS uses your CloudTrail events to identify the services and actions used and generate a least privileged policy that you can attach to this user.

Users > mtm\_user

### Summary

User ARN am:aws:iam:721254631510:user/mtm\_user Path / Creation time 2022-04-24 13:03 UTC+0530

Permissions Groups (1) Tags Security credentials Access Advisor

**Sign-in credentials**

Summary	• User does not have console management access • MFA is required when signing in. Learn more
Console password	Disabled   Manage
Assigned MFA device	am:aws:iam:721254631510:mfa/mtm_user (Virtual)   Manage
Signing certificates	None ↗

**Access keys**

Use access keys to make programmatic calls to AWS from the AWS CLI, Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time.

For your protection, you should never share your secret keys with anyone. As a best practice, we recommend frequent key rotation. If you lose or forget your secret key, you cannot retrieve it. Instead, create a new access key and make the old key inactive. Learn more

Create access key

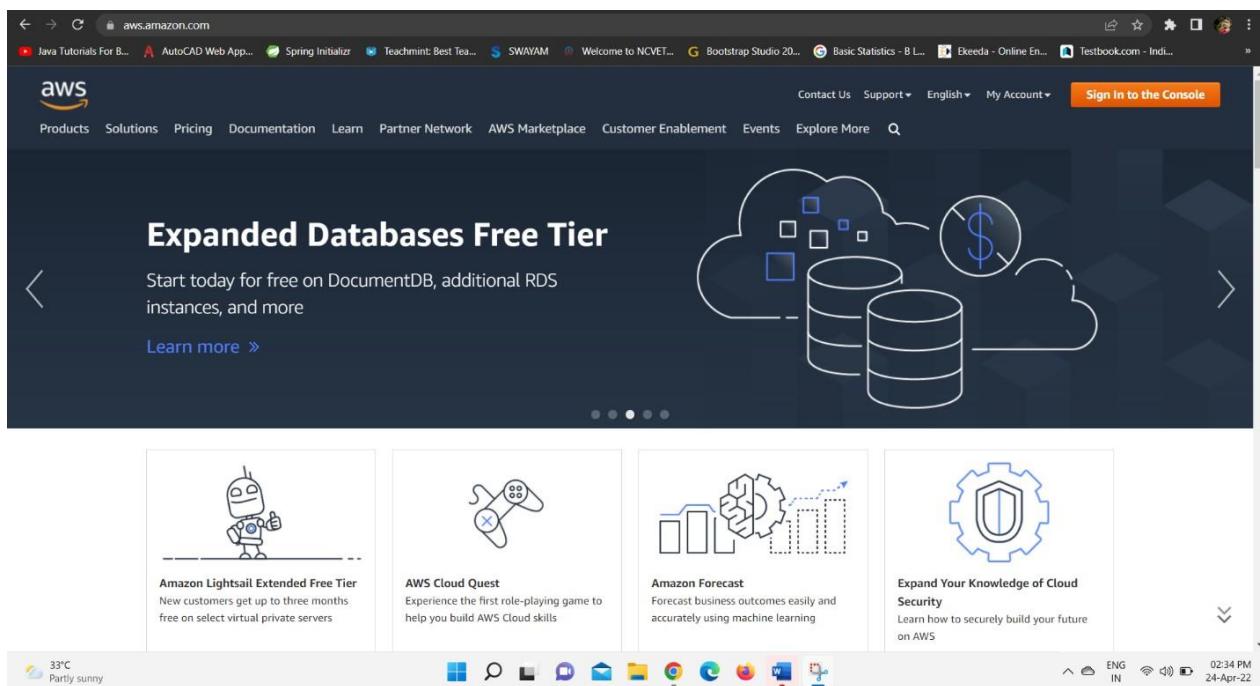
Access key ID	Created	Last used	Status
---------------	---------	-----------	--------

© 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms Cookie preferences

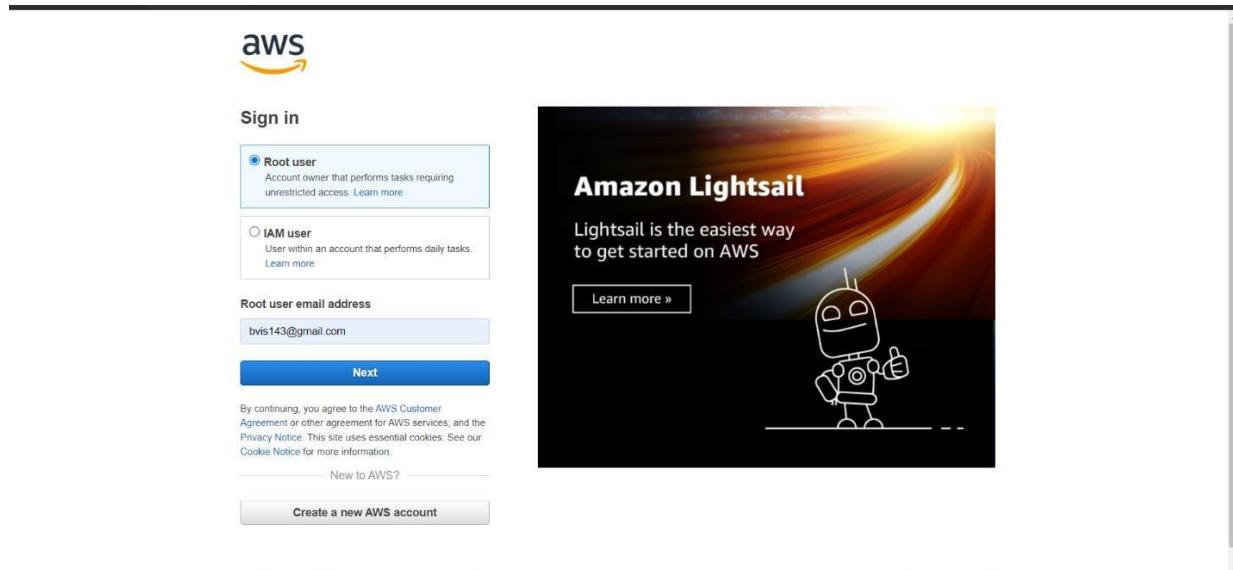
## EXPERIMENT NO 9

**Aim:** To study and Implement Security as a Service on AWS/Azure

### Step 1: Open the AWS Webpage



### Step 2: Sign up and Log in in AWS



The screenshot shows the AWS Management Console homepage. At the top, there's a search bar and a navigation bar with 'Services' selected. Below the search bar, the title 'AWS Management Console' is displayed. On the left, there's a sidebar titled 'AWS services' with sections for 'Recently visited services' (IAM, S3, EC2, RDS, Elastic Beanstalk) and 'All services'. The main content area features a section titled 'Build a solution' with four cards: 'Launch a virtual machine', 'Build a web app', 'Build using virtual servers', and 'Register a domain'. Below this are two more sections: 'Connect an IoT device' and 'Start migrating to AWS', each with its own card. To the right, there are promotional banners for 'New AWS Console Home', 'Stay connected to your AWS resources on-the-go', and 'Explore AWS'.

## Step 3: Go to Service & Search the IAM

The screenshot shows the AWS Management Console search results for 'IAM'. The search bar at the top contains 'IAM'. The results are categorized into 'Services' and 'Features'. Under 'Services', there are five items: IAM, Resource Access Manager, Amazon VPC IP Address Manager, and Serverless Application Repository. Under 'Features', there are four items: Groups, Roles, Policies, and Users. To the right of the search results, there are promotional banners for 'New AWS Console Home', 'Stay connected to your AWS resources on-the-go', and 'Explore AWS'.

## Step 4: Open the IAM dashboard

The screenshot shows the IAM dashboard. On the left, there's a sidebar with 'Identity and Access Management (IAM)' selected. The main dashboard has a header 'IAM dashboard' and 'Security recommendations'. It shows a red warning icon with the message 'Add MFA for root user'. Below this is a green checkmark with the message 'Root user has no active access keys'. There's also a section for 'IAM resources' with counts: 2 User groups, 4 Users, 7 Roles, 0 Policies, and 0 Identity providers. A 'What's new' section lists recent updates. On the right, there are sections for 'AWS Account' (Account ID: 721254631510, Account Alias: 721254631510), 'Quick Links' (My security credentials, Manage your access keys, multi-factor authentication (MFA) and other credentials), 'Tools' (Policy simulator, Web identity federation playground), and 'Additional information' (Best practices for Identity and Access Management).

## EXPERIMENT NO 10

### Step 1: Launch a EC2 Instance

The screenshot shows the AWS Management Console search results for the term 'ec'. The search bar at the top contains 'ec'. On the left, there is a sidebar with categories: Services (107), Features (218), Resources (New), Blogs (18,383), Documentation (229,403), Knowledge Articles (30), Tutorials (96), Events (651), and Marketplace (237). The main area displays a list of services under 'Services': EC2 (Virtual Servers in the Cloud), Security Hub (AWS's security and compliance center), Security Lake (Automatically centralize all your security data with a few clicks), and Direct Connect (Dedicated Network Connection to AWS). Below this, there is a section titled 'Features' with a 'See all 218 results' link.

### Step 2: click on instances -> Launch Instances

The screenshot shows the EC2 Management Console Instances page. The search bar at the top contains 'Search'. On the left, there is a sidebar with links: New EC2 Experience (Tell us what you think), EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (Instances Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), and Images. The main area displays a table of instances:

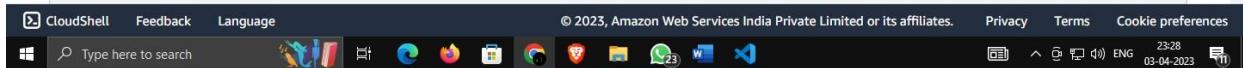
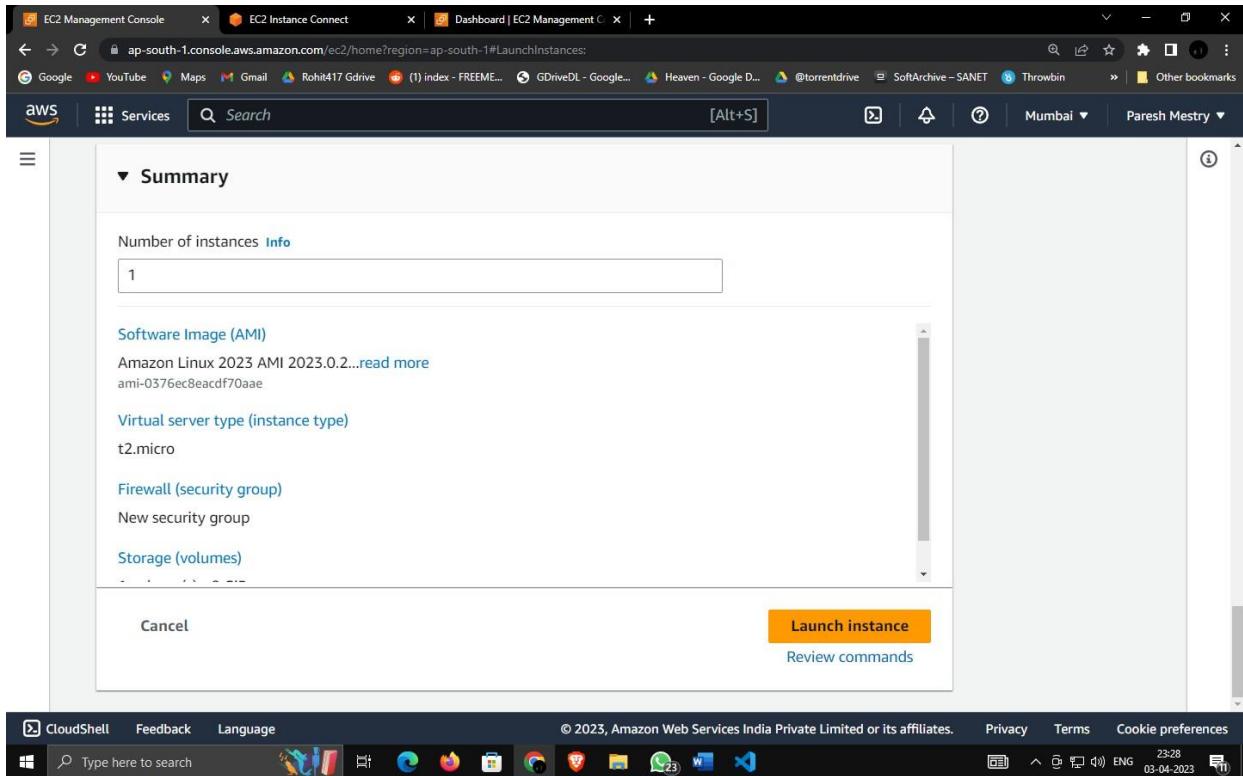
Name	Instance ID	Instance state	Instance type	Status check
ansibleNode	i-02bc2e468145208ff	Stopped	t2.micro	-
webapp	i-0d6e2178cef81f5d3	Running	t2.micro	Initializing

At the bottom, there is a detailed view for the instance 'i-0d6e2178cef81f5d3 (webapp)'. The status bar at the bottom right shows the date and time as 03-04-2023 23:24.

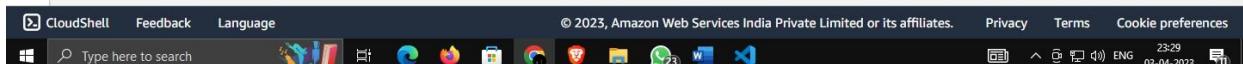
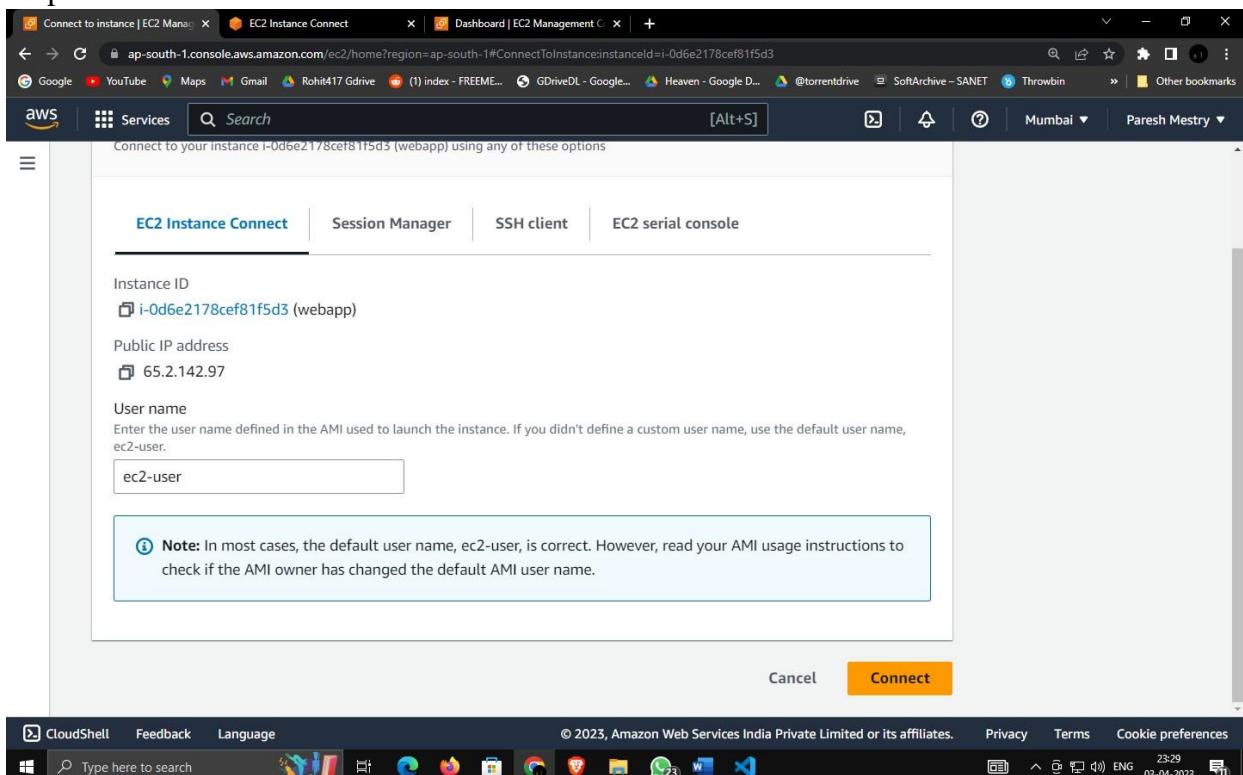
### Step 3: give name and select amazon Linux with proper configuration

The screenshot shows the AWS EC2 Management Console with a search bar containing 'webapp'. Below the search bar, there's a section titled 'Application and OS Images (Amazon Machine Image)'. It includes a search bar for 'Search our full catalog including 1000s of application and OS images'. Under the 'Recent' tab, there are icons for Amazon Linux, macOS, Ubuntu, Windows, Red Hat, and SUSE. A 'Quick Start' section highlights 'Amazon Linux 2023 AMI' as 'Free tier eligible'. The status bar at the bottom indicates it's from the AWS CloudShell.

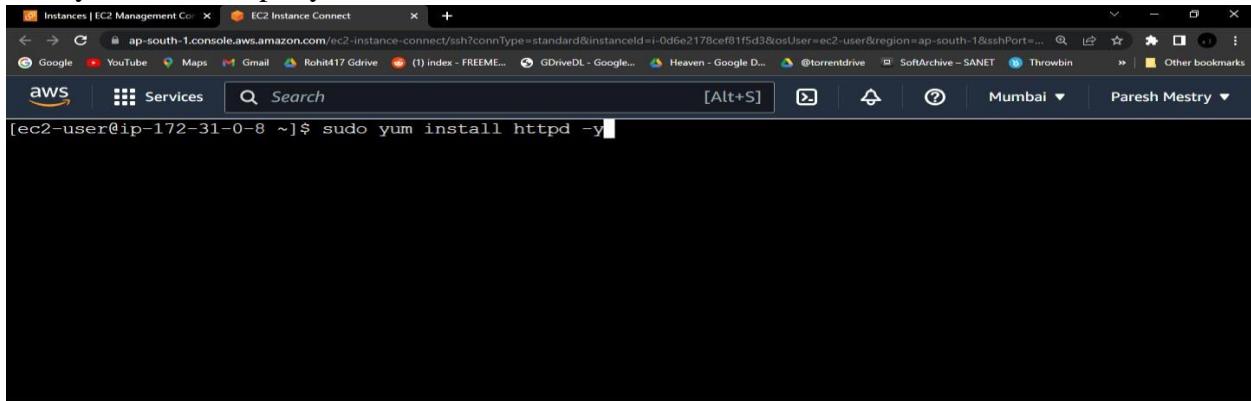
This screenshot shows the detailed view of the 'Amazon Linux 2023 AMI'. It lists the AMI ID as ami-0376ec8eacdf70aae (64-bit (x86), uefi-preferred) / ami-0405dec981e646696 (64-bit (Arm), uefi). It notes Virtualization: hvm, ENA enabled: true, and Root device type: ebs. The 'Verified provider' badge is present. Below this, the 'Instance type' section is shown, featuring the t2.micro instance type. The status bar at the bottom is identical to the one in the previous screenshot.



#### Step 4: Connect the Instance



Step 5: To host the website we need server for that we using Apache httpdInstall the httpd  
sudo yum install httpd -y



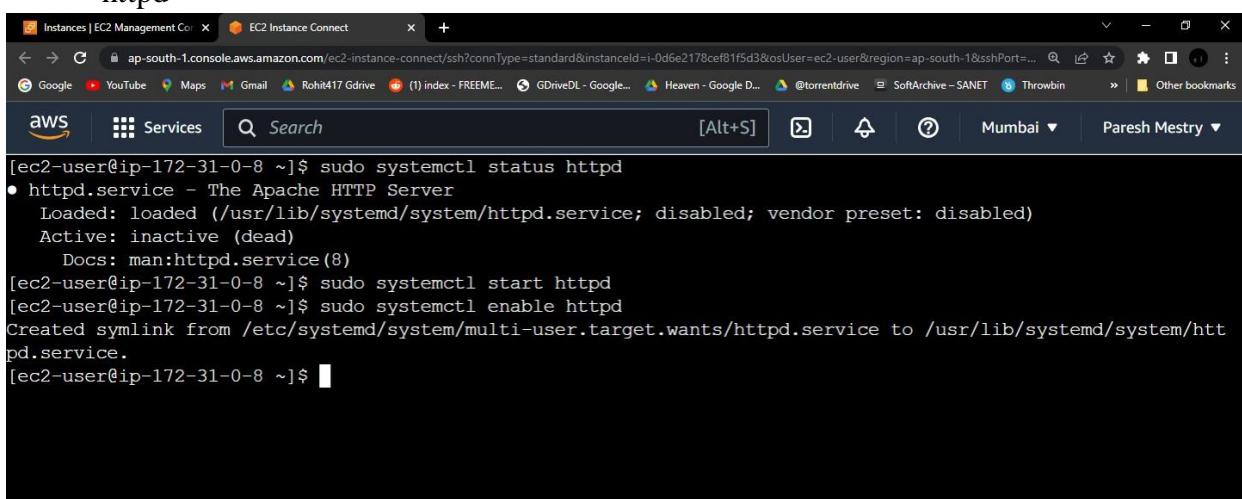
```
[ec2-user@ip-172-31-0-8 ~]$ sudo yum install httpd -y
```

i-0d6e2178cef81f5d3 (rhel)  
PublicIPs: 65.2.142.97 PrivateIPs: 172.31.0.8

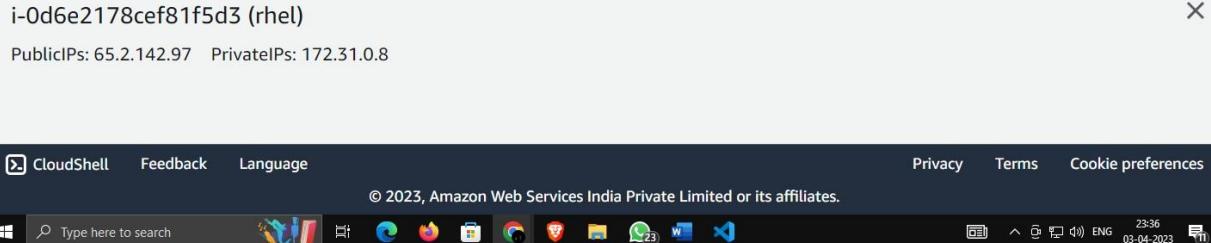
CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Step 6: start the httpd services and enable it on

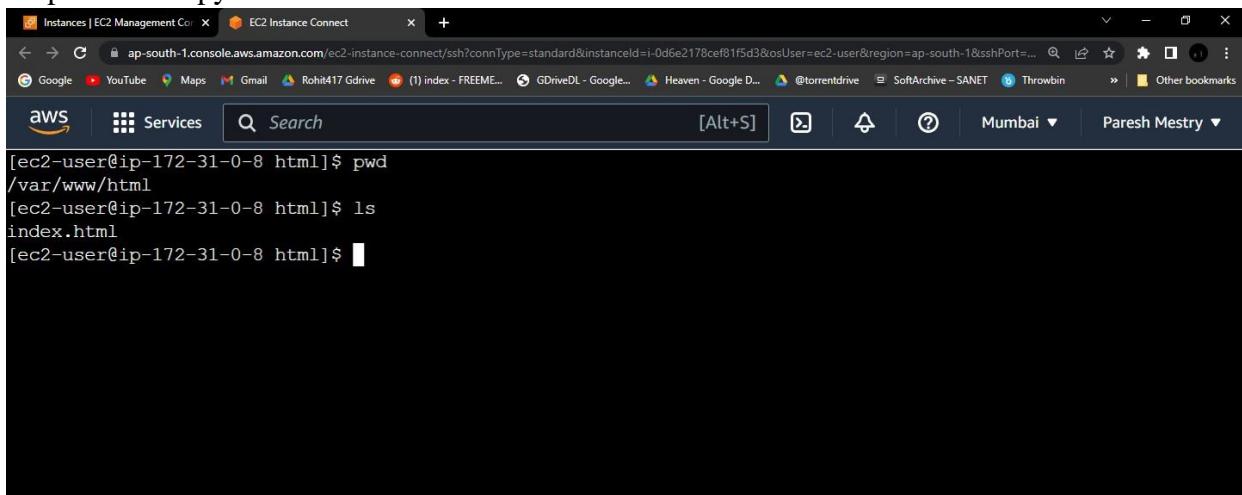
```
Startup.sudo systemctl status httpd  
sudo systemctl start httpd  
sudo systemctl enable  
httpd
```



```
[ec2-user@ip-172-31-0-8 ~]$ sudo systemctl status httpd  
● httpd.service - The Apache HTTP Server  
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)  
   Active: inactive (dead)  
     Docs: man:httpd.service(8)  
[ec2-user@ip-172-31-0-8 ~]$ sudo systemctl start httpd  
[ec2-user@ip-172-31-0-8 ~]$ sudo systemctl enable httpd  
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.  
[ec2-user@ip-172-31-0-8 ~]$
```



Step 7: now copy the website in /etc/var/www/html this folder



```
[ec2-user@ip-172-31-0-8 html]$ pwd  
/var/www/html  
[ec2-user@ip-172-31-0-8 html]$ ls  
index.html  
[ec2-user@ip-172-31-0-8 html]$
```

i-0d6e2178cef81f5d3 (webapp) X

PublicIPs: 65.2.142.97 PrivateIPs: 172.31.0.8

CloudShell Feedback Language Privacy Terms Cookie preferences

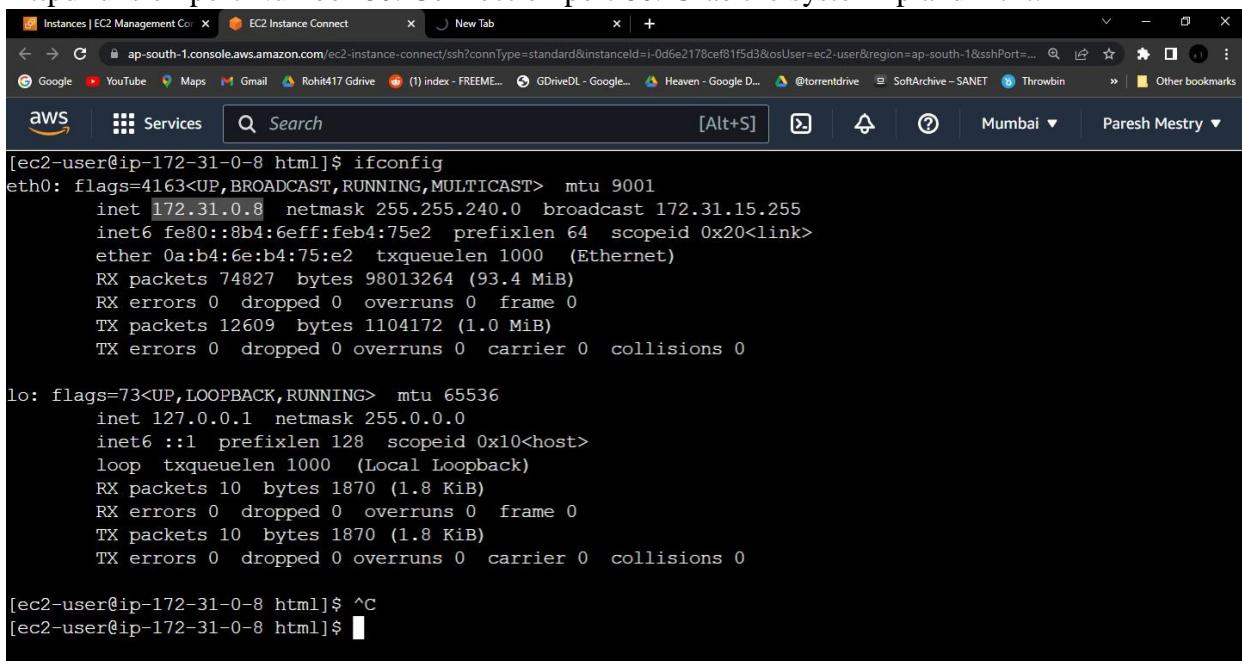
© 2023, Amazon Web Services India Private Limited or its affiliates.

Type here to search

23:51 03-04-2023

Step 8: now our website is on the server now check if it is working or not

Httpd runs on port Number 80. Connect on port 80. Grab the system Ip and hit it.



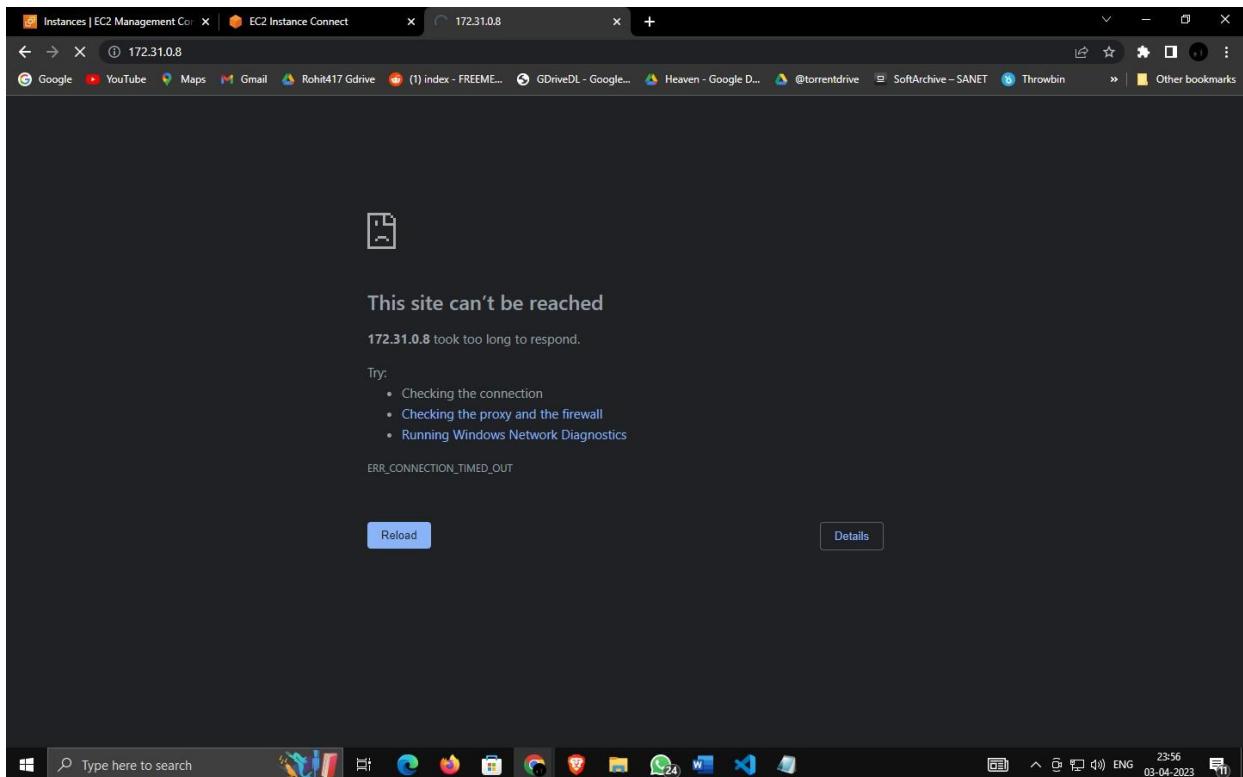
```
[ec2-user@ip-172-31-0-8 html]$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001  
      inet 172.31.0.8 netmask 255.255.240.0 broadcast 172.31.15.255  
      inet6 fe80::8b4:6eff:feb4:75e2 prefixlen 64 scopeid 0x20<link>  
      ether 0a:b4:6e:b4:75:e2 txqueuelen 1000 (Ethernet)  
      RX packets 74827 bytes 98013264 (93.4 MiB)  
      RX errors 0 dropped 0 overruns 0 frame 0  
      TX packets 12609 bytes 1104172 (1.0 MiB)  
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
      inet 127.0.0.1 netmask 255.0.0.0  
      inet6 ::1 prefixlen 128 scopeid 0x10<host>  
      loop txqueuelen 1000 (Local Loopback)  
      RX packets 10 bytes 1870 (1.8 KiB)  
      RX errors 0 dropped 0 overruns 0 frame 0  
      TX packets 10 bytes 1870 (1.8 KiB)  
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
[ec2-user@ip-172-31-0-8 html]$ ^C  
[ec2-user@ip-172-31-0-8 html]$
```

CloudShell Feedback Language Privacy Terms Cookie preferences

© 2023, Amazon Web Services India Private Limited or its affiliates.

Type here to search

23:55 03-04-2023



Looks like our website not working because. to connect from the outside world we need to connect onsystems public Ip

Go on security tab and set inbound rule.

A screenshot of the AWS EC2 Management Console. The left sidebar shows navigation options like 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', and 'Instances'. Under 'Instances', 'Instances' is selected, showing a list of 2 instances: 'ansibleNode' (Stopped) and 'webapp' (Running). The 'Security' tab is selected for the 'webapp' instance. The 'Security details' section shows the IAM Role is '-' and the Owner ID is '170261483583'. The Launch time is 'Mon Apr 03 2023 23:24:57 GMT+0530 (India Standard Time)'. The security group assigned is 'sg-0d193d4af6d36e7cb (launch-wizard-3)'. The browser's taskbar at the bottom shows various pinned icons and the date/time '03-04-2023 23:59'.

Click on edit inbound rule -> add rule add All traffic rule from anywhere.

The screenshot shows the AWS EC2 Management Console. On the left, there's a sidebar with links like EC2 Dashboard, EC2 Global View, Events, Tags, and Limits. Under Instances, there are links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, and Capacity Reservations. The main area shows the EC2 Instance Connect interface. At the top, it says "Inbound rules count: 1 Permission entry". Below that, there are tabs for Inbound rules, Outbound rules, and Tags. A message box says "You can now check network connectivity with Reachability Analyzer" with a "Run Reachability Analyzer" button. The Inbound rules table shows one row:

<input checked="" type="checkbox"/>	Name	Security group rule...	IP version	Type
<input checked="" type="checkbox"/>	-	sgr-0688197a5f191dc42	IPv4	SSH

The screenshot shows the "Edit inbound rules" wizard. At the top, it says "Edit inbound rules" and "Info". Below that, it says "Inbound rules control the incoming traffic that's allowed to reach the instance." The main area shows the "Inbound rules" table with two rows:

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-0688197a5f191dc42	SSH	TCP	22	Custom	0.0.0.0 / 0
-	All traffic	All	All	Anywh...	0.0.0.0 / 0

At the bottom, there are buttons for "Add rule", "Cancel", "Preview changes", and "Save rules". The status bar at the bottom indicates "00:01 04-04-2023".

Now Try again with public Ip Now It's Working.

