

Mihir Jawale
240840325033

Cloud

Step 1 In the dashboard click on IAM .

The screenshot shows the AWS IAM Dashboard. On the left, a sidebar menu includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings), and 'Access reports' (Access Analyzer, External access, Unused access, Analyzer settings, Credential report). The main content area displays 'Security recommendations' with two items: 'Root user has MFA' (Having multi-factor authentication (MFA) for the root user improves security for this account) and 'Root user has no active access keys' (Using access keys attached to an IAM user instead of the root user improves security). Below this is the 'IAM resources' section, which lists User groups (0), Users (0), Roles (2), Policies (0), and Identity providers (0). To the right, there are three panels: 'AWS Account' (Account ID: 686255971493, Account Alias: Create, Sign-in URL: https://686255971493.signin.aws.amazon.com/console), 'Quick Links' (My security credentials), and a footer with CloudShell, Feedback, and system status (3°C Haze).

Step 2 After that click on user in that click on 'create user'

The screenshot shows the AWS IAM service in the AWS Management Console. The left sidebar is titled 'Identity and Access Management (IAM)' and includes sections for Dashboard, Access management (User groups, Users, Roles, Policies, Identity providers, Account settings), and Access reports (Access Analyzer, External access, Unused access, Analyzer settings, Credential report). The main content area is titled 'Users (0) Info' and contains a table with one row, indicating 'No resources to display'. At the top right of the table, there is a 'Create user' button, which is circled in red. The browser address bar shows the URL: us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users.

3 Give it a name

The screenshot shows the 'Create user' wizard in the AWS IAM service. The current step is 'Step 1 Specify user details'. The title is 'Specify user details'. On the left, there are three navigation options: 'Step 2 Set permissions' (disabled), 'Step 3 Review and create' (disabled), and 'Step 1 Specify user details' (selected). The main form is titled 'User details' and contains a 'User name' field with the value 'newuser1'. Below the field, a note states: 'The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . @ _ - (hyphen)'. There is also an optional checkbox 'Provide user access to the AWS Management Console - optional' with a note: 'If you're providing console access to a person, it's best practice [link] to manage their access in IAM Identity Center.' At the bottom right of the form are 'Cancel' and 'Next' buttons, with 'Next' being highlighted in orange. The browser address bar shows the URL: us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/create.

4 After that attach the policy directly
Search for ec2 and s3

The screenshot shows the 'Create user | IAM | Global' step 3: 'Review and create' page. It displays the user details and permissions summary.

User details:

User name: newuser1	Console password type: None	Require password reset: No
---------------------	-----------------------------	----------------------------

Permissions summary:

Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy
AmazonEC2FullAccess	AWS managed	Permissions policy
AmazonS3FullAccess	AWS managed	Permissions policy

Tags - optional: Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

5 After that go to the 'newuser1' user dashboard and click on security credentials

Identity and Access Management (IAM)

newuser1 [Info]

Summary

ARN arn:aws:iam::686255971493:user/newuser1	Console access Disabled	Access key 1 Create access key
Created October 21, 2024, 16:46 (UTC+05:30)	Last console sign-in -	

Permissions | Groups | Tags | Security credentials | Last Accessed

Console sign-in

Console sign-in link https://686255971493.signin.aws.amazon.com/console	Console password Not enabled
---	---------------------------------

Multi-factor authentication (MFA) (0)

CloudShell Feedback

CloudShell Feedback

31°C Haze

6 After that click on enable control access

Click on auto generate password for the user console access

Identity and Access Management (IAM)

Console access enabled.

Console password

You have successfully enabled the user's new password.
This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

Console sign-in link
<https://686255971493.signin.aws.amazon.com/console>

User name
newuser1

Console password
LnCj0@O[Hide

Download .csv file Close

Manage console access

16:49 GMT+5:30

Remove Resync Assign MFA device

Each user can have a maximum of 8 MFA devices assigned. Learn more

Created on 21-10-2024

Assign MFA device

CloudShell Feedback

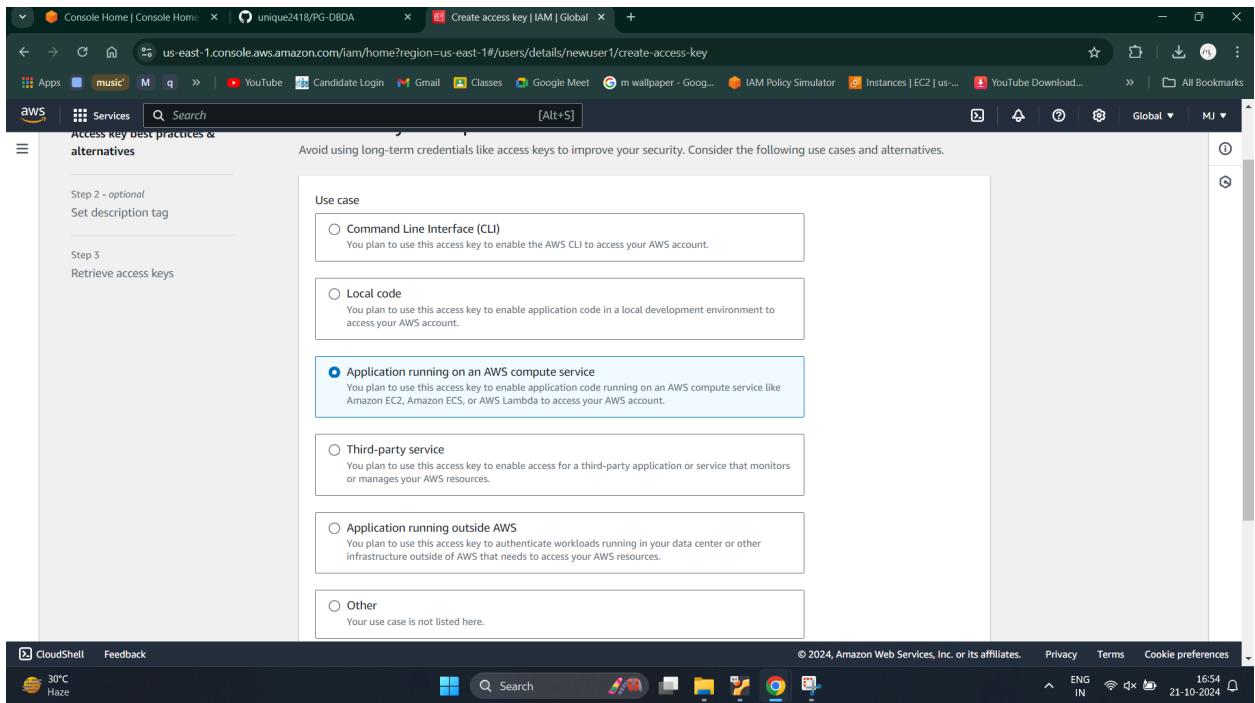
CloudShell Feedback

31°C Haze

7 After that create access key to access the bucket

In this console click the “Application running on an aws computer service”

Click confirm and next



8 give this a tag name and then click on create on create access key and download the csv file

Console Home | Console Home | Create access key | IAM | Global

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/users/details/newuser1/create-access-key

Create access key | IAM | Global

Access key created

This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

Step 1: Access key best practices & alternatives

Step 2 - optional: Set description tag

Step 3: Retrieve access keys

Retrieve access keys

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIAZ7SALDSSTGR2BHOI	***** Show

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

Download .csv file Done

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 16:53 21-10-2024

9 Login in using the credentials of new user

Console Home | Console Home | Amazon Web Services Sign-In

eu-north-1.sigin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2fcanvas&code_challenge=4dvFoxdR0mIT7ChrKx0IMctAS_GccEckdZvcasVhS... Incognito

Try the new sign in UI See our new improved Amazon Web Services sign in experience before we officially launch. Enable new sign in

aws

Sign in as IAM user

Account ID (12 digits) or account alias: 686255971493

IAM user name: newuser1

Password:

Remember this account

Sign in

Sign in using root user email
Forgot password?

Amazon Lightsail

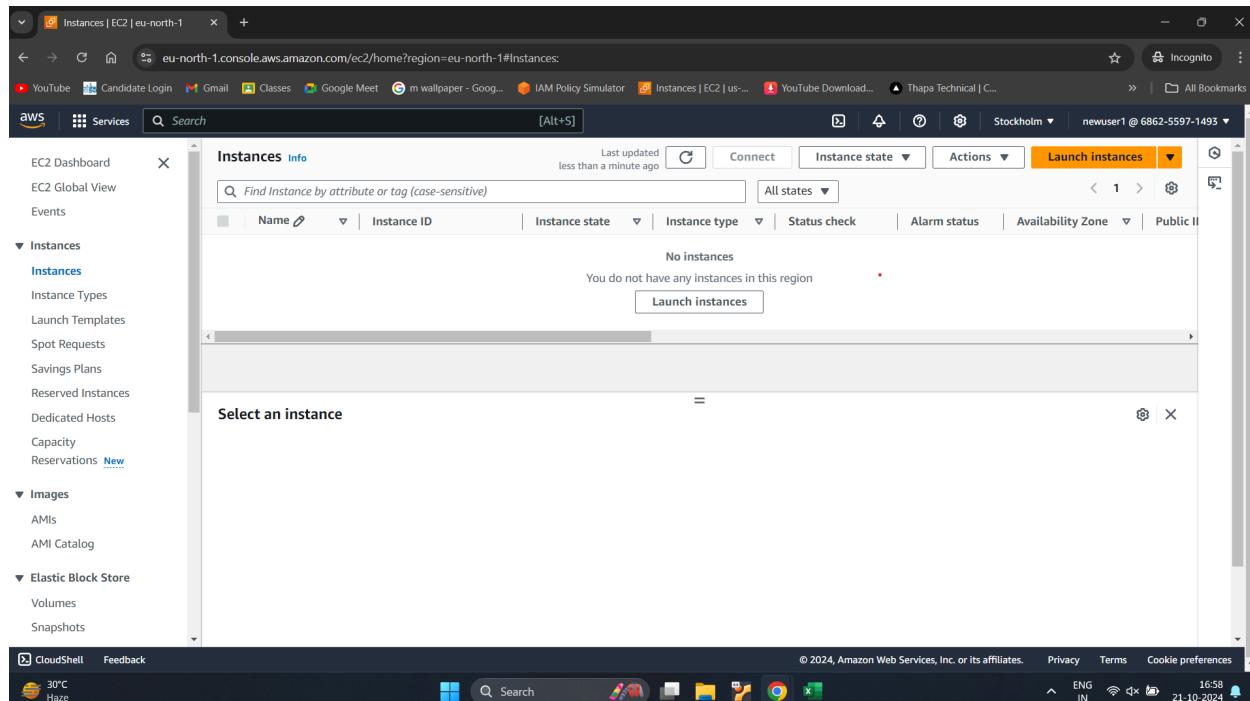
Lightsail is the easiest way to get started on AWS

Learn more »

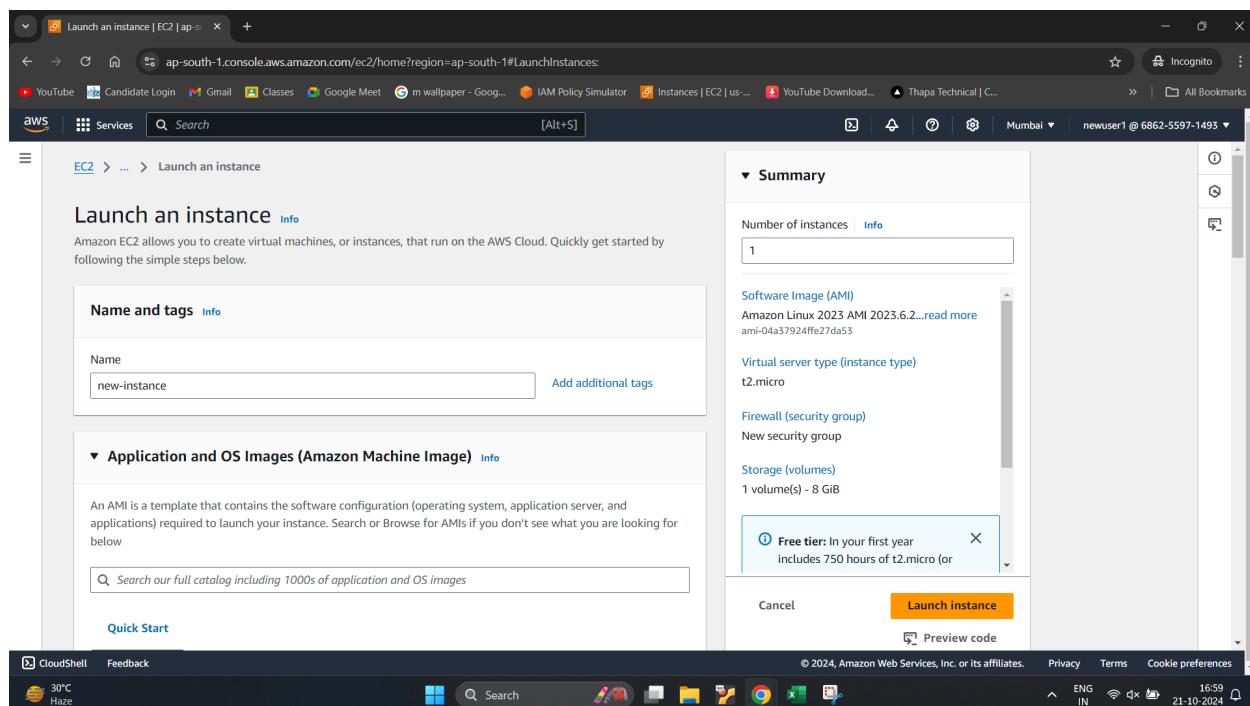
30°C Haze

ENG IN 16:56 21-10-2024

10 after that create a new instance under the button launch instance



In that put a name after that use the key created earlier.



Check the 2 option

The screenshot shows the AWS EC2 Launch Instance wizard. In the 'Key pair (login)' section, there is a dropdown menu labeled 'Select' with an empty search bar. Below it, a note says 'Proceed without a key pair (Not recommended)'. A 'Create new key pair' button is visible. To the right, a summary panel shows 'Number of instances: 1' and 'Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...'. A tooltip for the free tier is displayed: 'Free tier: In your first year includes 750 hours of t2.micro (or'. A large orange 'Launch instance' button is prominent.

The screenshot shows the AWS EC2 Launch Instance wizard. In the 'Firewall (security group)' section, there are two options: 'Create security group' (radio button selected) and 'Select existing security group'. Below, under 'Additional charges apply when outside of free tier allowance', three checkboxes are checked: 'Allow SSH traffic from Anywhere', 'Allow HTTPS traffic from the internet', and 'Allow HTTP traffic from the internet'. A red circle highlights the 'Allow HTTP traffic from the internet' checkbox. A tooltip for the free tier is displayed: 'Free tier: In your first year includes 750 hours of t2.micro (or'. A summary panel on the right shows 'Number of instances: 1' and 'Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2...'. A large orange 'Launch instance' button is present.

11 Here our instance is running

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with options like EC2 Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity, Reservations, Images, AMIs, AMI Catalog, and Elastic Block Store. The main content area has a title 'Instances (1) Info' and a table with one row. The row contains 'Name' (new-instance), 'Instance ID' (i-03c84a78e10aa61db), 'Instance state' (Running), 'Status check' (Initializing), 'Alarm status' (View alarms), 'Availability Zone' (ap-south-1b), and 'Public IP' (ec2-13-232-140-37.ap-south-1.compute.amazonaws.com). Below the table is a section titled 'Select an instance'.

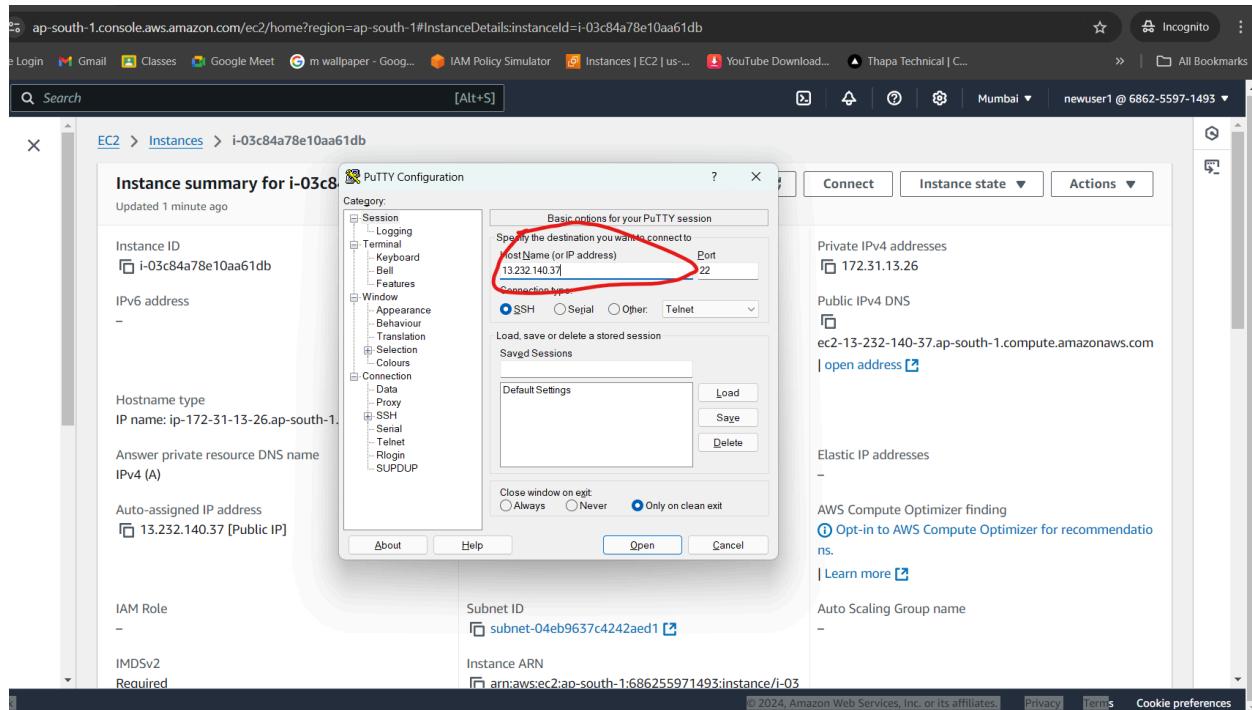
12 copy the public address to start putty

The screenshot shows the AWS EC2 Instance details page for the instance 'i-03c84a78e10aa61db'. The left sidebar is identical to the previous screenshot. The main content area has a title 'Instance summary for i-03c84a78e10aa61db (new-instance) Info' and a note 'Updated less than a minute ago'. It displays various instance details: Instance ID (i-03c84a78e10aa61db), IPv6 address (none), Instance state (Running), Hostname type (IP name: ip-172-31-13-26.ap-south-1.compute.internal), IP name (ip-172-31-13-26.ap-south-1.compute.internal), Answer private resource DNS name (IPv4 (A)), Auto-assigned IP address (13.232.140.37 [Public IP]), IAM Role (none), IMDSv2 Required, Private IP DNS name (ip-172-31-13-26.ap-south-1.compute.internal), Instance type (t2.micro), VPC ID (vpc-09140a7a7059e1456), Subnet ID (subnet-04eb9637c4242aed1), Instance ARN (arn:aws:ec2:ap-south-1:686255971493:instance/i-03c84a78e10aa61db), and Auto Scaling Group name (none). A red circle highlights the 'Public IPv4 address copied' message and the '13.232.140.37 | open address' link. To the right, there are sections for Private IPv4 addresses (172.31.13.26), Public IPv4 DNS (ec2-13-232-140-37.ap-south-1.compute.amazonaws.com), and Elastic IP addresses (none). At the bottom, there are links for AWS Compute Optimizer finding (Opt-in to AWS Compute Optimizer for recommendations) and Auto Scaling Group name.

13 click on start and paste the public address there

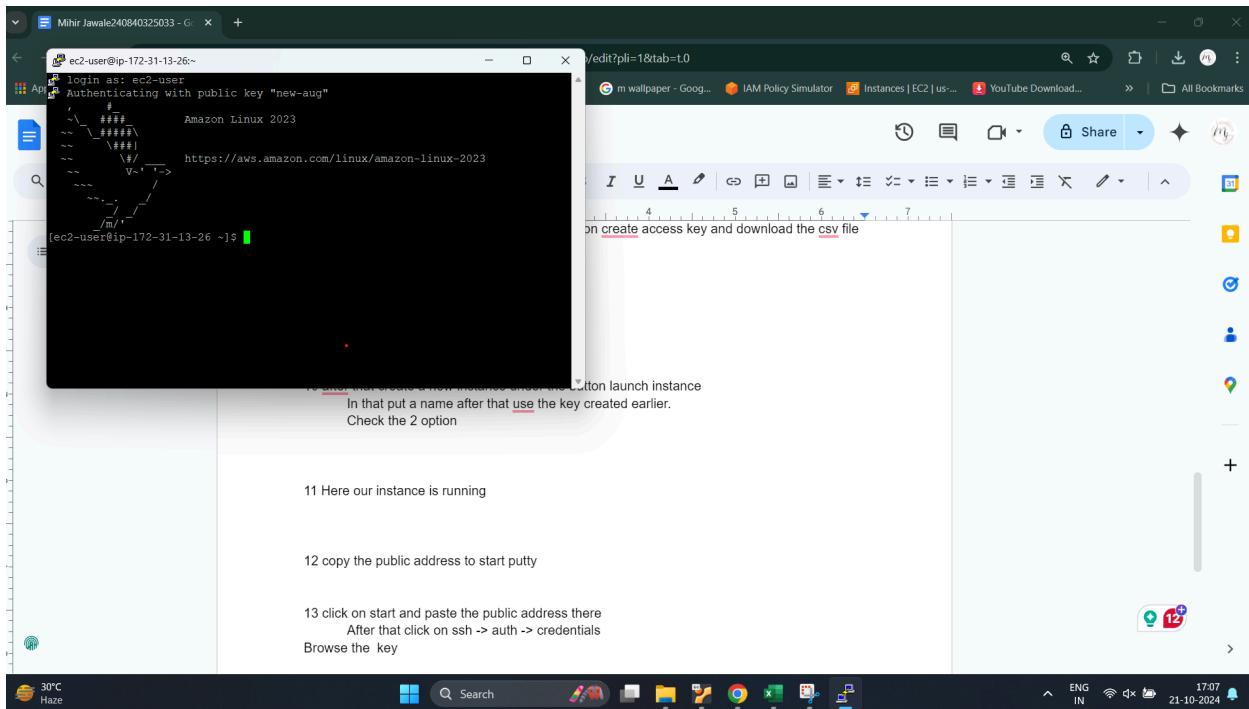
After that click on ssh -> auth -> credentials

Browse the key

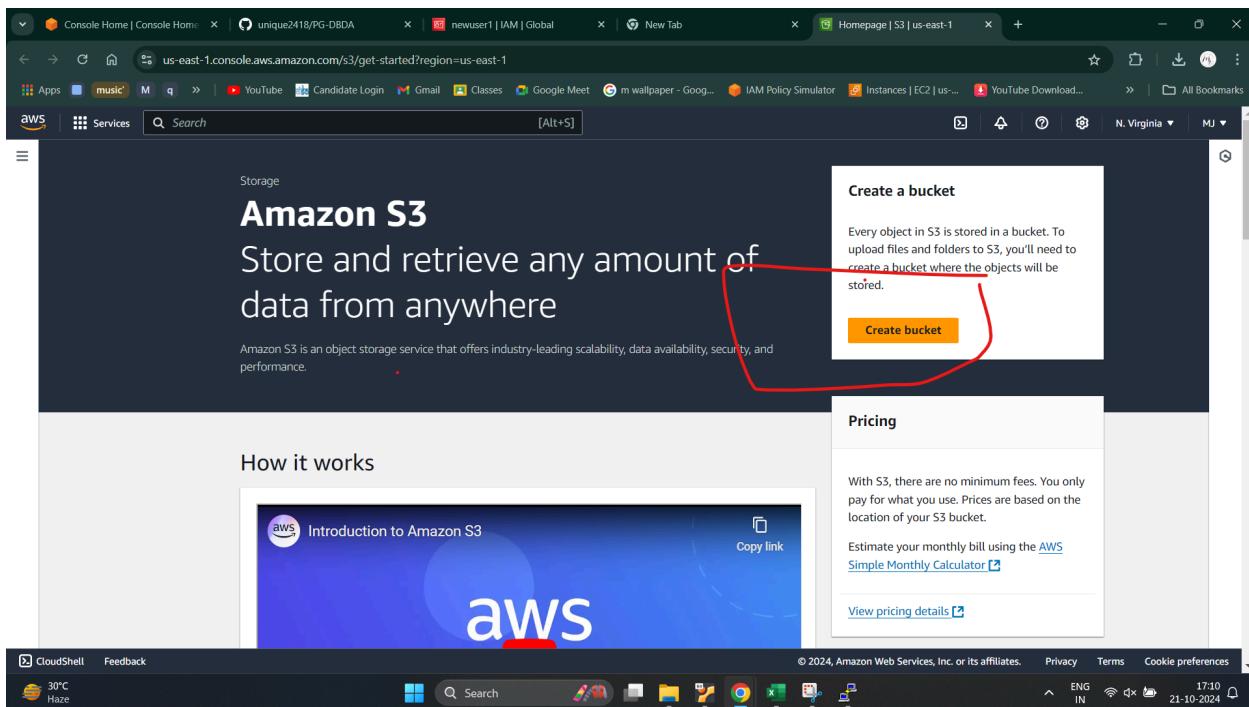


14 after that write 'ec2-user' to start

Then create a index.html file in that write **Hello, Welcome to my page**



15 Create a bucket in root user to upload the file index .html



In s3 click the create bucket in that give name to bucket

The screenshot shows the 'Create S3 bucket' page in the AWS Management Console. In the 'Object Ownership' section, the 'ACLs enabled' option is selected, indicated by a blue border around the radio button. A note below states: 'Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.' A warning message in a yellow box says: '⚠️ We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.' At the bottom of the ownership section, the 'Bucket owner preferred' option is selected.

The acls option to be enabled
Uncheck the public access

The screenshot shows the 'Create S3 bucket' page with the 'Block Public Access settings for this bucket' section expanded. The 'Block all public access' checkbox is checked, indicated by a blue border around it. A note below says: 'Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.' Below this are four unchecked checkboxes: 'Block public access to buckets and objects granted through new access control lists (ACLS)', 'Block public access to buckets and objects granted through any access control lists (ACLS)', 'Block public access to buckets and objects granted through new public bucket or access point policies', and 'Block public and cross-account access to buckets and objects through any public bucket or access point policies'. A warning message in a yellow box says: '⚠️ Turning off block all public access might result in this bucket and the objects within becoming public. AWS recommends that you turn on block all public access, unless public access is required for specific and verified use cases such as static website hosting.' At the bottom of the page, there is a checkbox for acknowledging the warning message.

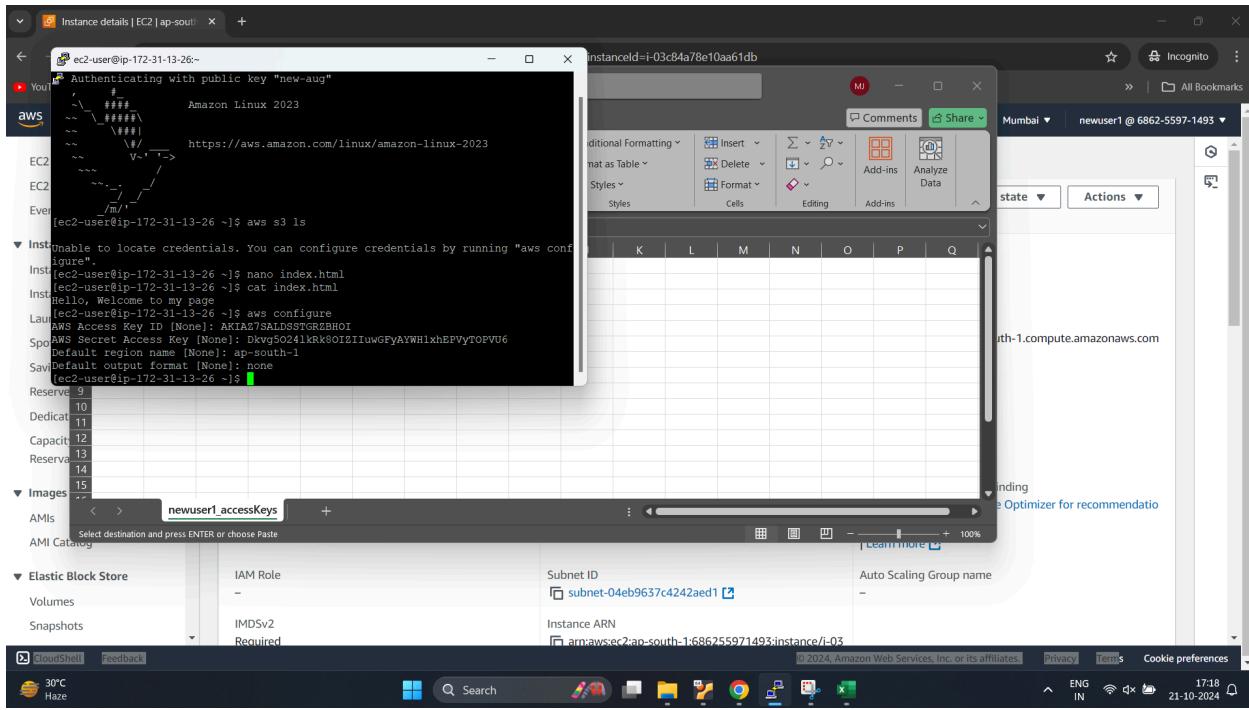
16 Bucket created

The screenshot shows the AWS S3 console with a green success message at the top: "Successfully created bucket \"new-bucketmk\"". Below it, there's a link to "View details". The main interface shows an "Account snapshot" with an update frequency of "updated every 24 hours" and a "View Storage Lens dashboard" button. Under "General purpose buckets", there is one entry: "new-bucketmk" (US East (N. Virginia) us-east-1). A "Create bucket" button is visible at the top right of the list.

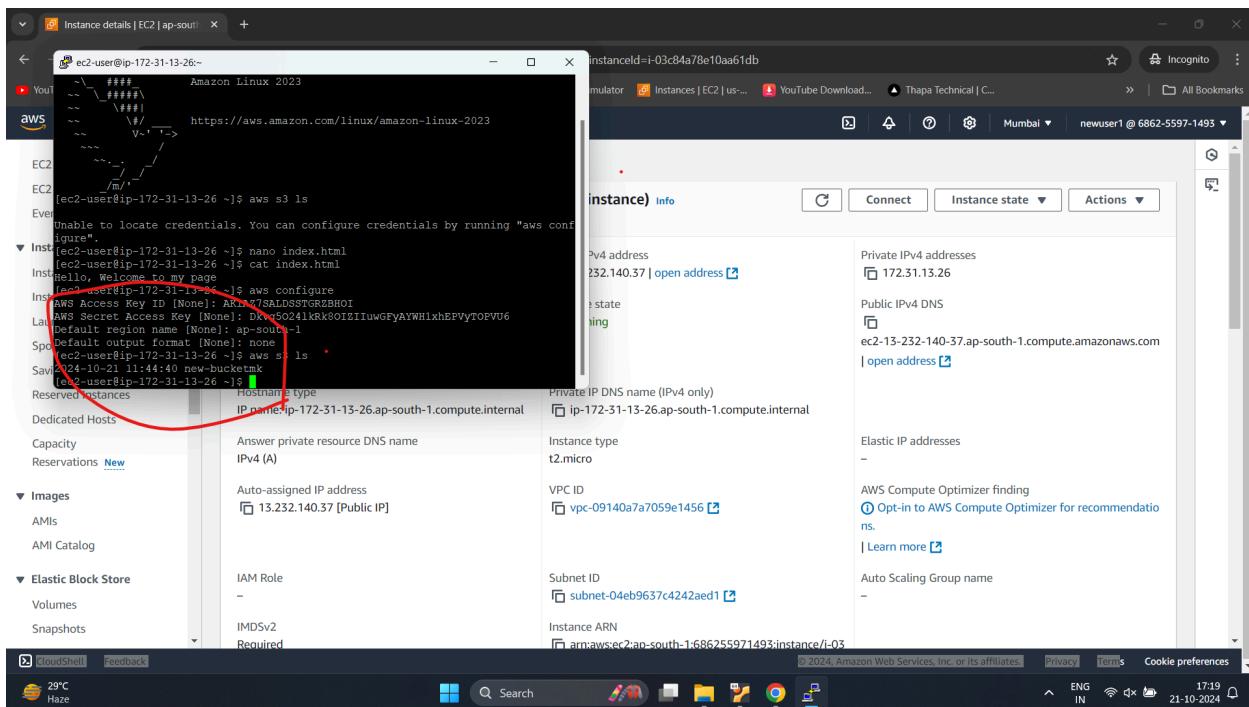
17 Under properties option scroll down and click on Static website enabled

The screenshot shows the "Edit static website hosting - S3" configuration page. Under "Static website hosting", the "Enable" option is selected. Under "Hosting type", the "Host a static website" option is selected. A note states: "For your customers to access content at the website endpoint, you must make all your content publicly readable. To do so, you can edit the S3 Block Public Access settings for the bucket. For more information, see Using Amazon S3 Block Public Access." Below this, there are fields for "Index document" (set to "index.html") and "Error document - optional" (set to "error.html"). At the bottom, there's a section for "Redirection rules - optional". The status bar at the bottom indicates "CloudShell Feedback" and the date "21-10-2024".

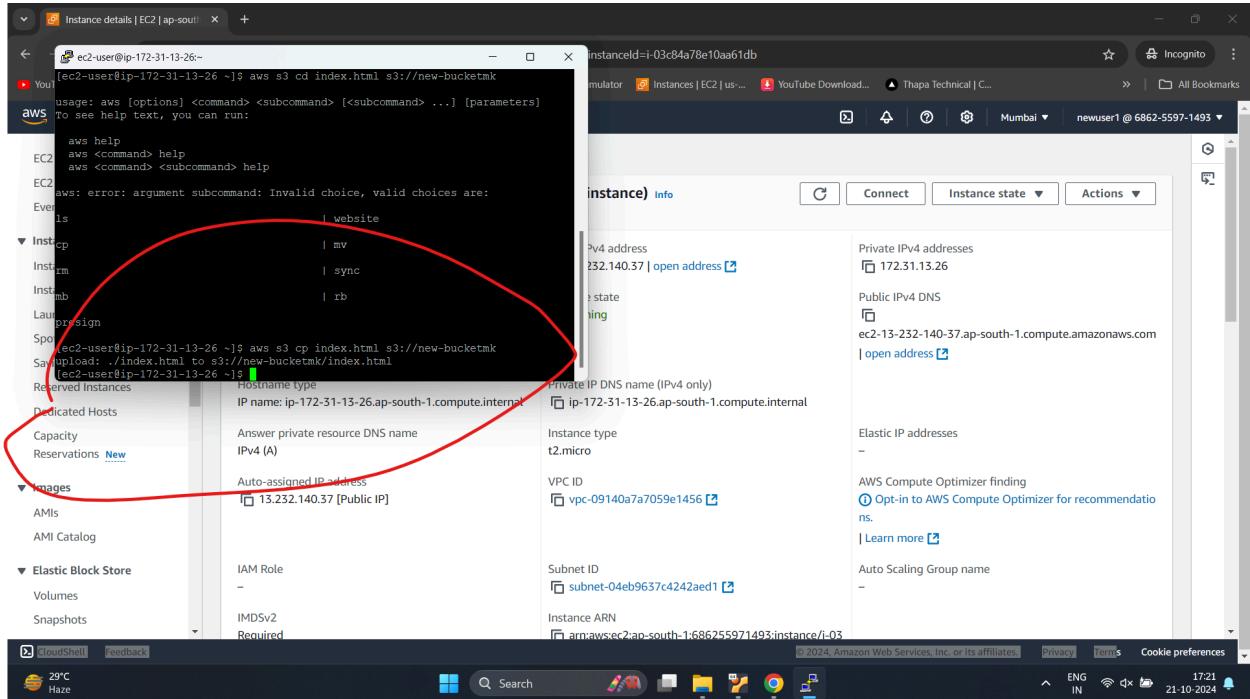
18 after that go on putty and configure the aws using aws configure
Give the acces key and secret access key



19 using aws s3 ls the bucket has been listed



20 After that using the command "aws s3 cp index.html s3://new-bucketmk" the file has been uploaded



21 Goes to the bucket to check for the file

The screenshot shows the AWS S3 console interface. On the left, a sidebar titled 'Amazon S3' lists various options like Buckets, Storage Lens, and Feature spotlight. The main area displays a bucket named 'new-bucketmk'. Under the 'Objects' tab, there is one item: 'index.html' (Type: html). The object was last modified on October 21, 2024, at 17:21:43 (UTC+05:30), and has a size of 26.0 B, stored in the Standard storage class. A search bar and a 'Show versions' button are also present. The 'Actions' menu is open, showing options such as Copy, Move, Initiate restore, Query with S3 Select, Edit actions, Rename object, Edit storage class, Edit server-side encryption, Edit metadata, Edit tags, and Make public using ACL.

22 select the bucket and click on actions after that click on make public acl and click on make public

This screenshot is identical to the one above, showing the AWS S3 console with the 'new-bucketmk' bucket. The 'Actions' menu is open over the 'index.html' object. The 'Make public using ACL' option is highlighted with a blue border, indicating it is the selected action.

The screenshot shows the 'Amazon S3 > Buckets > new-bucketmk > Make public' dialog. It displays a table of 'Specified objects' with one item: 'index.html' (html, 26.0 B). A warning message states: 'When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.' A large orange 'Make public' button is at the bottom right.

Specified objects

Name	Type	Last modified	Size
index.html	html	October 21, 2024, 17:21:43 (UTC+05:30)	26.0 B

Cancel Make public

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 29°C Haze ENG IN 17:24 21-10-2024

The screenshot shows the 'Amazon S3 > Buckets > new-bucketmk > Make public' dialog. It displays a table of 'Specified objects' with one item: 'index.html' (html, 26.0 B). A warning message states: 'When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.' A large orange 'Make public' button is at the bottom right.

Specified objects

Name	Type	Last modified	Size
index.html	html	October 21, 2024, 17:21:43 (UTC+05:30)	26.0 B

Cancel Make public

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 29°C Haze ENG IN 17:24 21-10-2024

23 Open the file after that click on the object url and copy it
And then open it in new browser

The screenshot shows the AWS S3 console interface. In the top navigation bar, there are several tabs including 'Console Home | Console', 'unique2418/PG-DBDA', 'newuser1 | IAM | Global', 'New Tab', 'index.html - Object in S3 b...', 'new-bucketmk.s3...', and 'new-bucketmk.s3...'. Below the tabs, the URL is 'us-east-1.console.aws.amazon.com/s3/object/new-bucketmk?region=us-east-1&bucketType=general&prefix=index.html'. The main content area shows the 'index.html' object details. The 'Properties' tab is selected. The 'Object overview' section displays the following information:

Owner	S3 URI
mihir12242002	s3://new-bucketmk/index.html
AWS Region	Amazon Resource Name (ARN)
US East (N. Virginia) us-east-1	arn:aws:s3:::new-bucketmk/index.html
Last modified	Entity tag (Etag)
October 21, 2024, 17:21:43 (UTC+05:30)	4775d0bc143cd53342c62e57ea8c26ed
Size	Object URL
26.0 B	https://new-bucketmk.s3.amazonaws.com/index.html
Type	
html	

At the bottom of the page, there are links for 'CloudShell', 'Feedback', and the AWS logo. The status bar at the bottom right shows 'ENG IN' and the date '21-10-2024'.

24 The html has been successfully uploaded and open

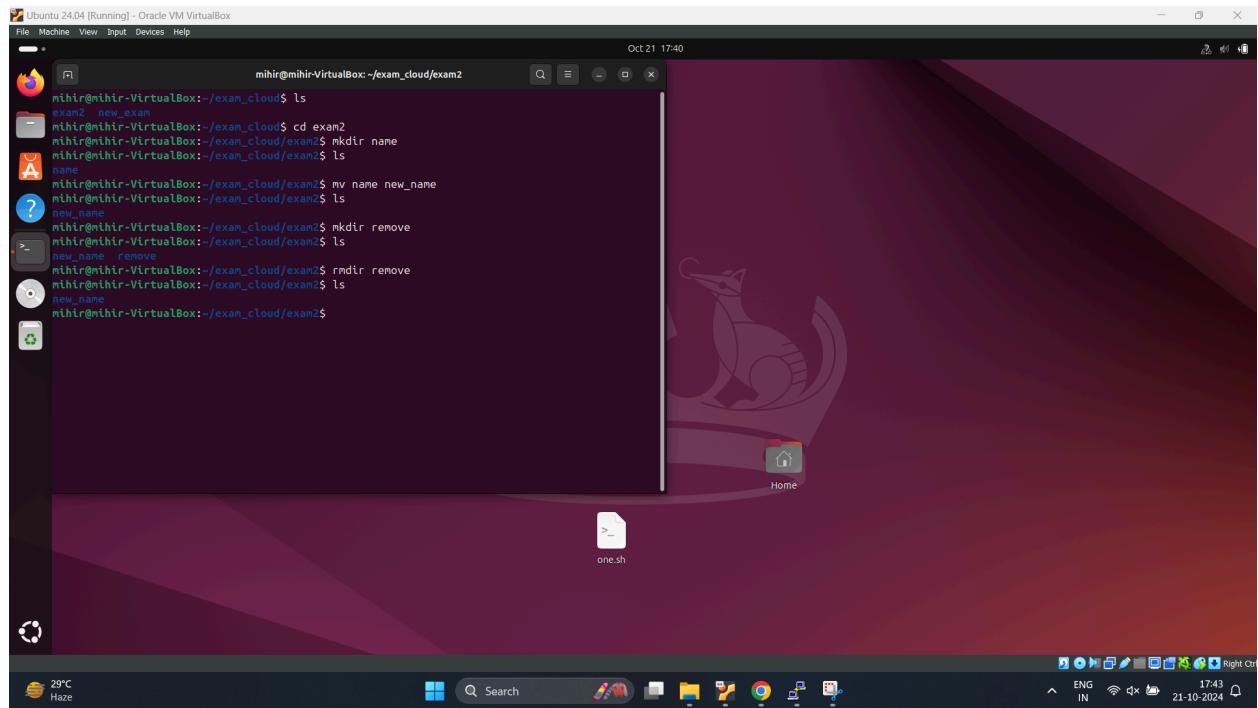
The screenshot shows a web browser window with the URL 'new-bucketmk.s3.amazonaws.com/index.html'. The page content is 'Hello, Welcome to my page'. At the top of the browser window, there are several tabs including 'Console Home | Console', 'unique2418/PG-DBDA', 'newuser1 | IAM | Global', 'New Tab', 'index.html - Object in S3 b...', 'new-bucketmk.s3...', and 'new-bucketmk.s3...'. The browser's address bar also shows 'new-bucketmk.s3.amazonaws.com/index.html'. The status bar at the bottom right shows 'ENG IN' and the date '21-10-2024'.

The link for the file is

<https://new-bucketmk.s3.amazonaws.com/index.html>

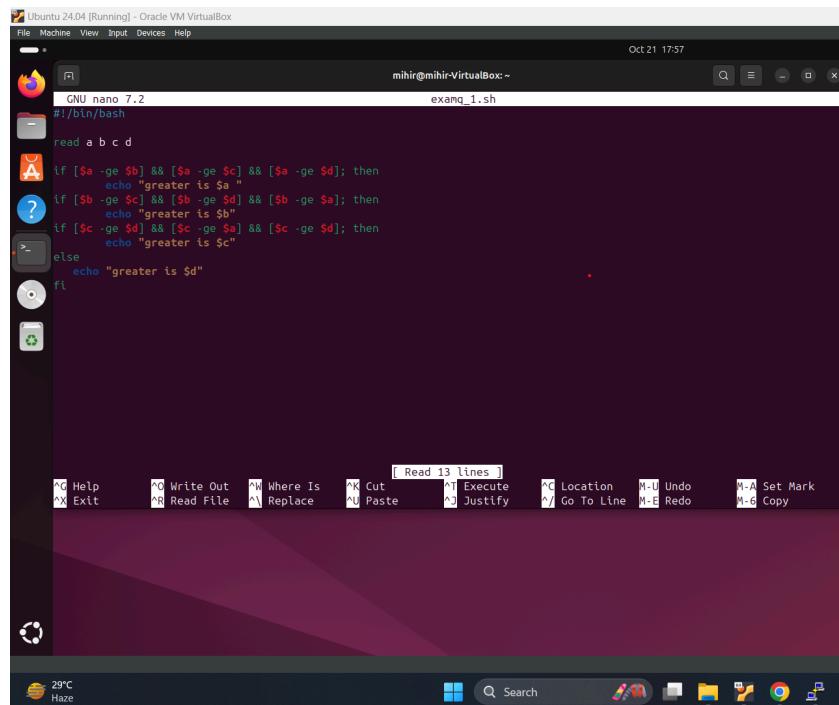
Linux

Q.2



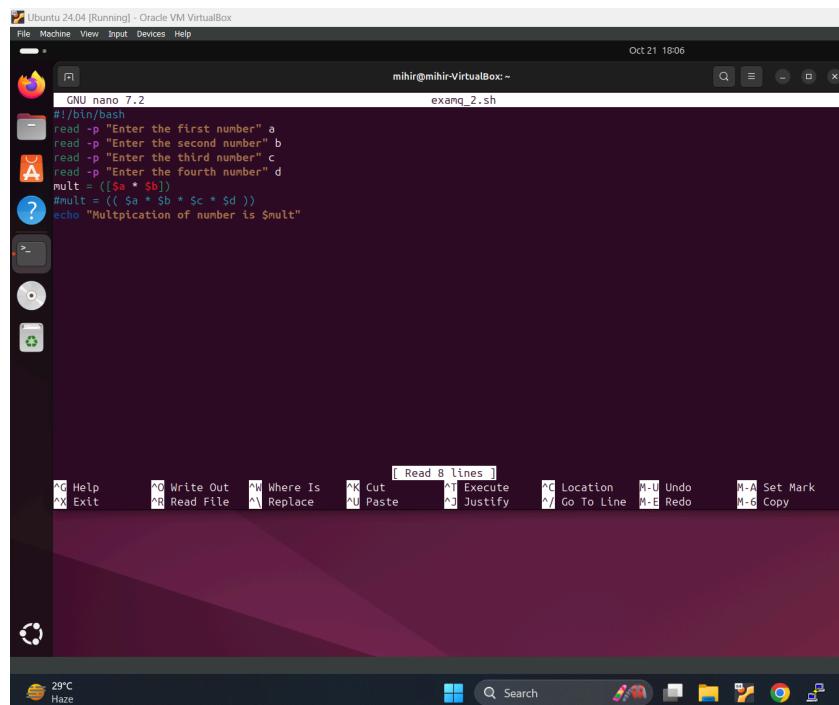
Q,1

a) Largest number



```
GNU nano 7.2          examq_1.sh
#!/bin/bash
read a b c d
if [ $a -ge $b ] && [ $a -ge $c ] && [ $a -ge $d ]; then
    echo "greater is $a"
elif [ $b -ge $c ] && [ $b -ge $d ] && [ $b -ge $a ]; then
    echo "greater is $b"
elif [ $c -ge $d ] && [ $c -ge $a ] && [ $c -ge $b ]; then
    echo "greater is $c"
else
    echo "greater is $d"
fi
```

b) Product



```
GNU nano 7.2          examq_2.sh
#!/bin/bash
read -p "Enter the first number" a
read -p "Enter the second number" b
read -p "Enter the third number" c
read -p "Enter the fourth number" d
mult = ($(a * $b))
#mult = (( $a * $b * $c * $d ))
echo "Multiplication of number is $mult"
```