Hindi Vidya Prachar Samiti's

Ramniranjan Jhunjhunwala College of Arts,

Science & Commerce (Autonomous),

Ghatkopar(W) MUMBAI - 400 086

DEPARTMENT OF INFORMATION TECHNOLOGY

2022 - 2023

M.Sc. (I.T.) SEM III

Cloud Solution Architect - AWS

Name: Pavan Ashok Yadav

Roll No.: 620

INDEX

7	**Introduction to AWS Device Farm** A. Locate or Download an Example Android * .apk and iOS *. ipa File B. Upload and Test the Example Application C. Run Test and View the Run's Results	10/08/2022	127-138
8	**Case Study's** A. ABP News B. Buzzdial C. Classle D. LIFEPLATE	17/08/2022	139-148
9	**Amazon WorkDocs**	23/08/2022	149-152
10	**Managing Virtual Private Cloud** A. Creating VPC in AWS Cloud B. Creating and Adding Private Subnet in the Existing VPC C. Deleting VPC	24/08/2022	153-158

Practical 1: Getting Familiarized with AWS Console

A. Creating Aws Free Tier Account

B. Getting Familiarized with The Aws Console

A] Creating an AWS Account – A Step by Step Process

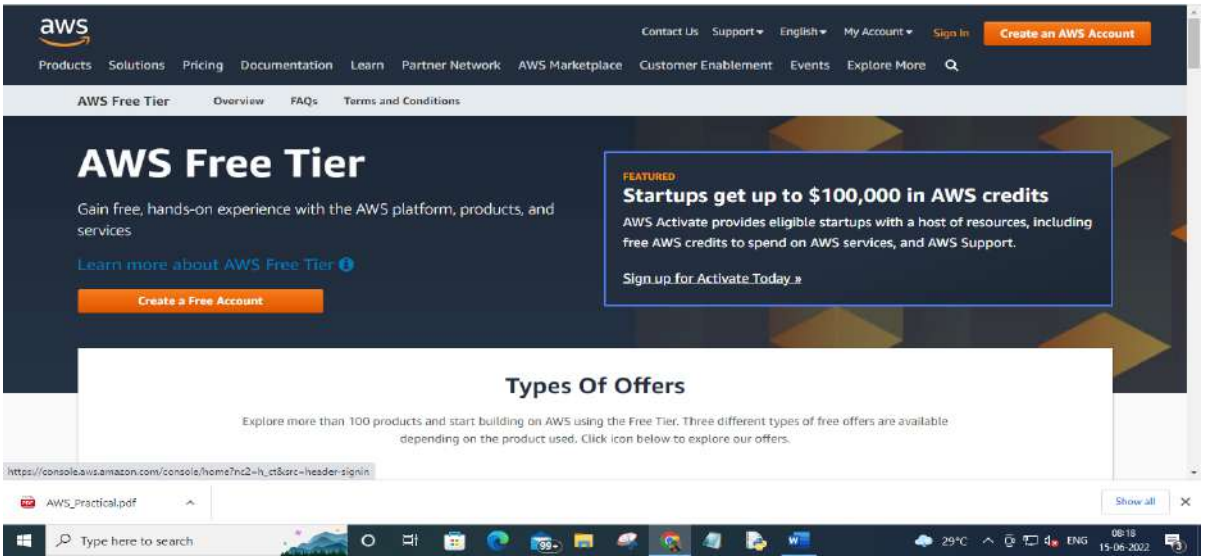
Creating an AWS Account is the first step you need to take in order to learn Amazon Web Services. Signing up for AWS provides you with all the tools you require to become an AWS professional.

In this practical, we will look at the step-by-step process of Creating an AWS Account.

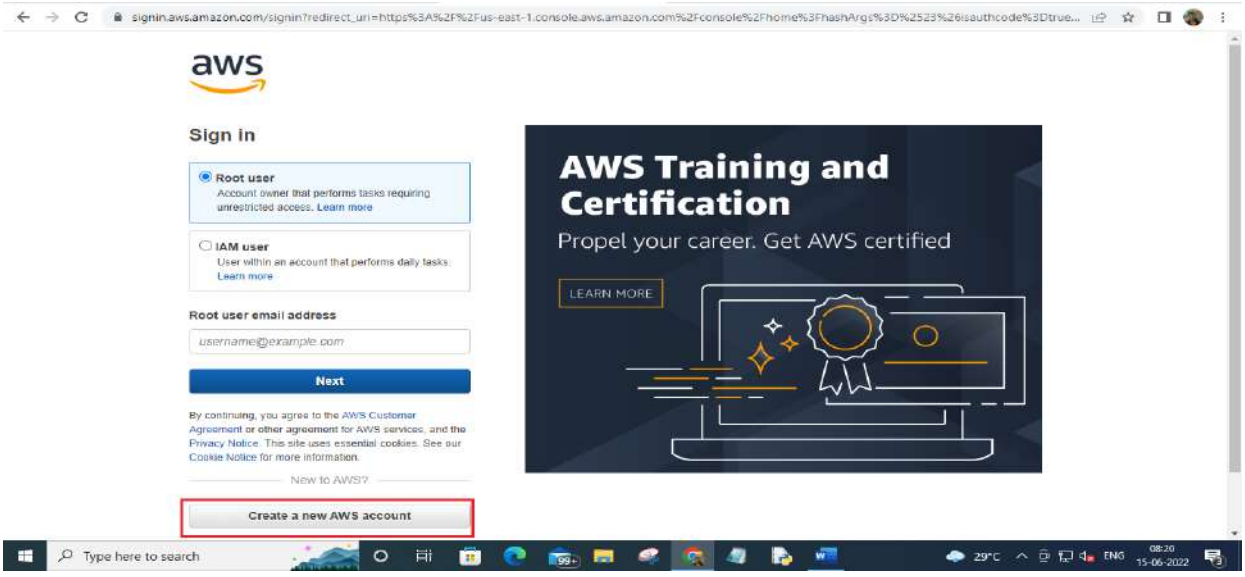
Step 1 – Visiting the Signup Page

Head over to the Amazon Web Services website for Creating an AWS Account.

You should see something like below:



In order to continue, click the **Sign In** button in the middle of the screen or on the top right corner of the screen. You will see the below screen.



If you are an existing user, you can sign in. Or you can click on the **Create a new AWS account** button. On this screen, you can also select your language preference from the dropdown below.

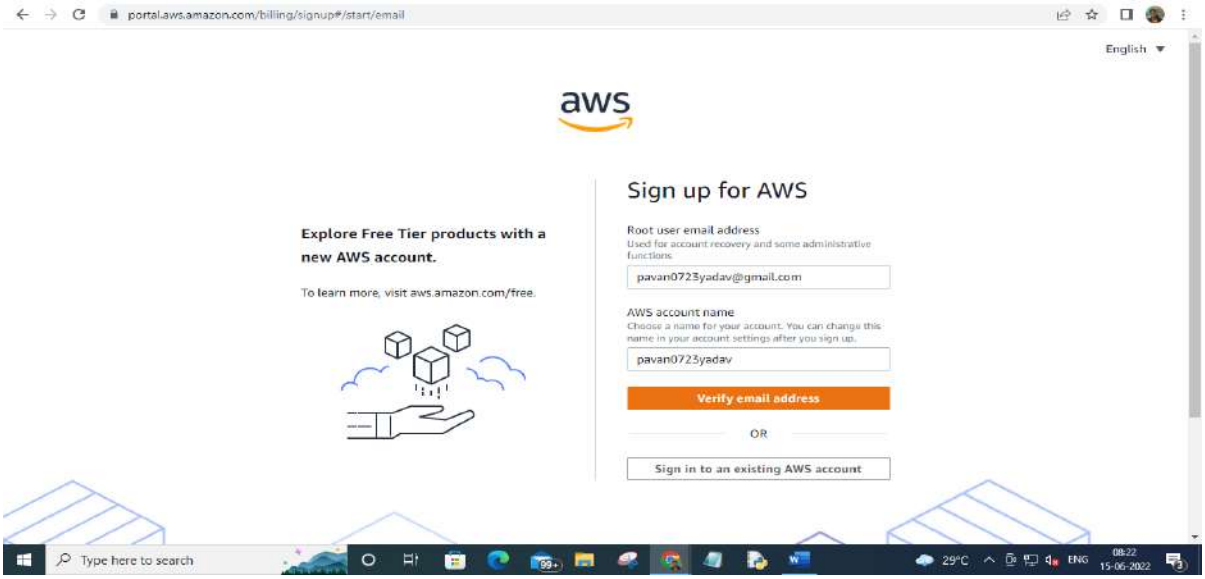
Step 2 – Entering User Details

After you have chosen to Create a new AWS account, you will see the below screen asking for few details

Root user email address: pavan0723yadav@gmail.com

AWS account name: pavan0723yadav

After that verify the email click on the **Verify email address** button



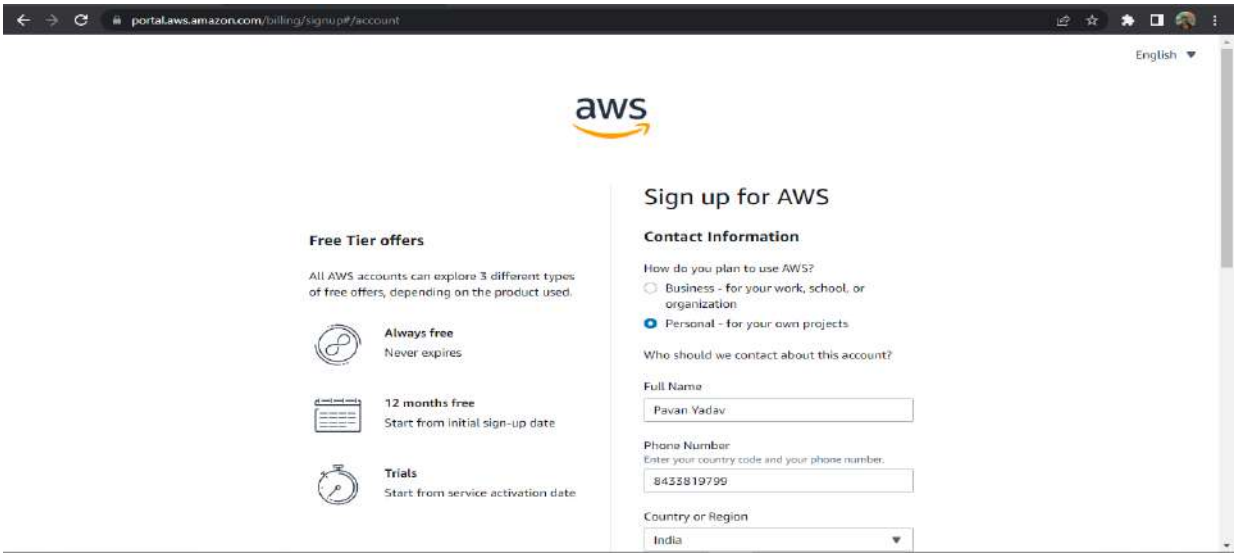
You can fill up the details as per your requirements and click Continue.

Next you will be asked to fill up your contact details such contact number, country, address and so on. You should fill them up properly because your contact number is important for further steps.

Password: P@v@nK0723

Step 3 – Entering User Details

After you have chosen to Create a new AWS account, you will see the below screen asking for few details.

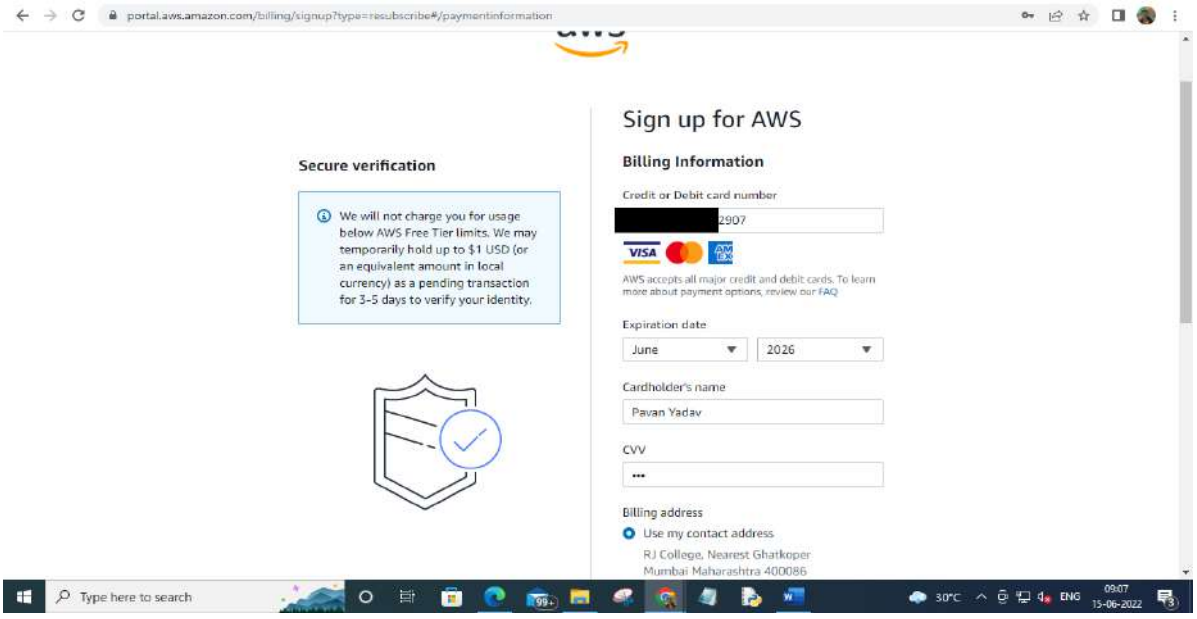


However, don't worry. This will not charge anything from your account (except for a verification amount that will be refunded back). But this is required in case you exceed the free-tier limit available with a new AWS Account.

After entering the details, click on Secure Submit button. It might take a while to process the request depending on your bank/credit card company servers.

Step 4 – Identity Confirmation

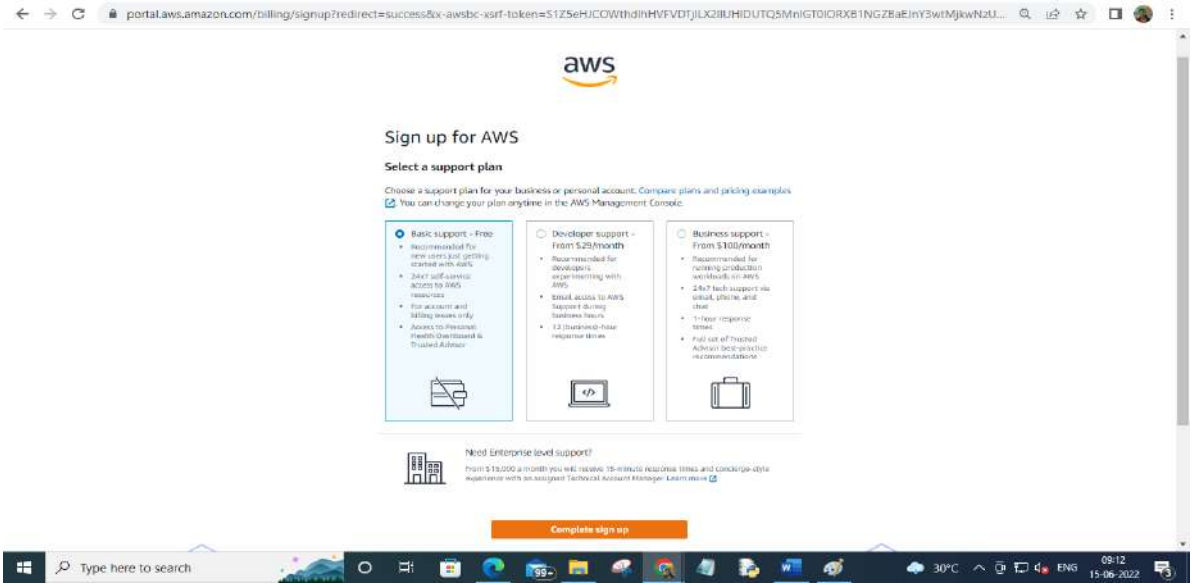
Once the credit card details are confirmed, you will need to complete the Identity Confirmation step. You will see the below screen:

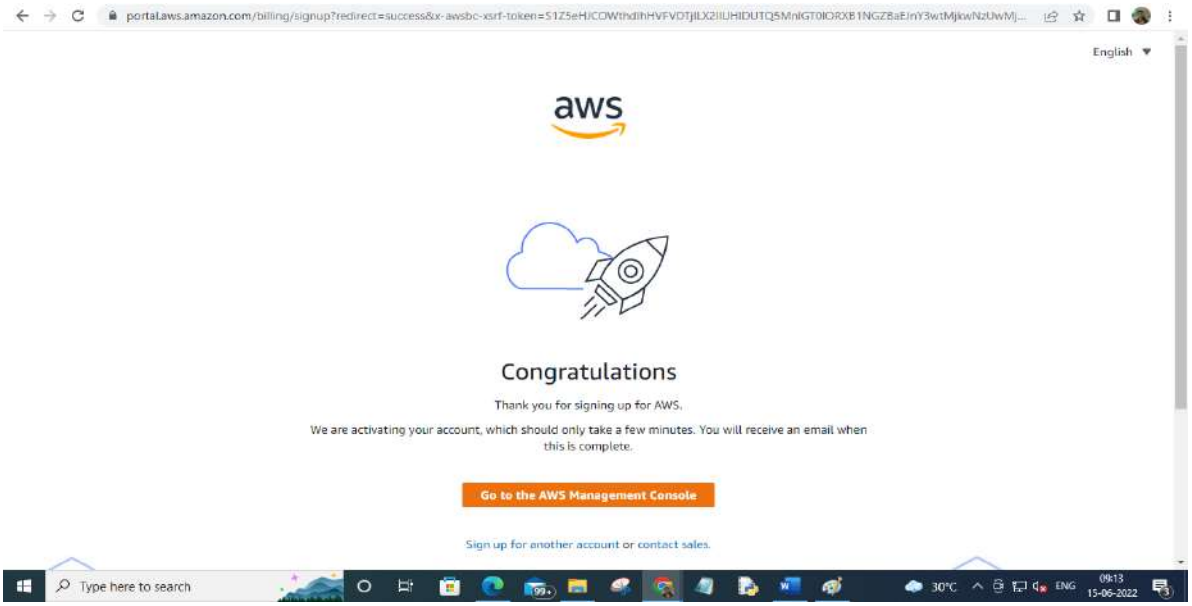


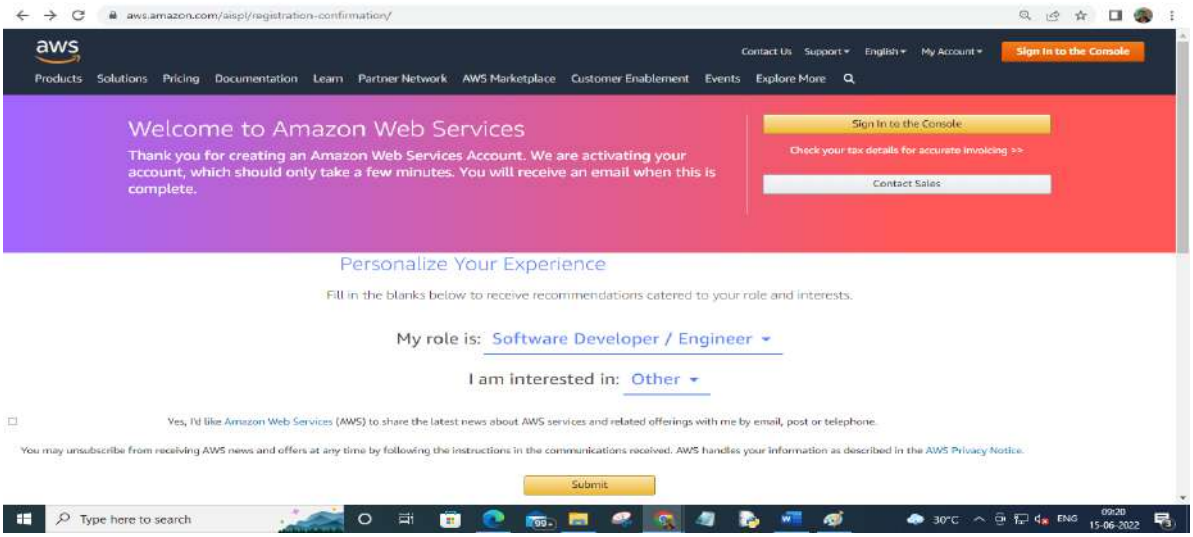
Basically, you need to select a mode to confirm your identity. It could be a Text Message or a Voice call to your valid phone number.

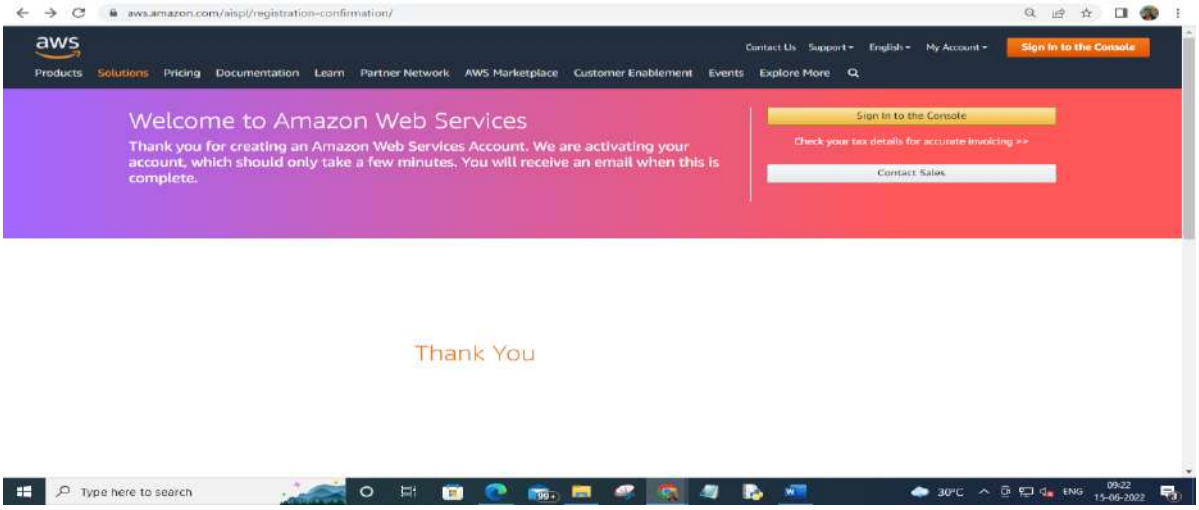
Step 5 – Selecting a Support Plan

In the next step for creating an AWS Account, we need to select the plan for our AWS Account.



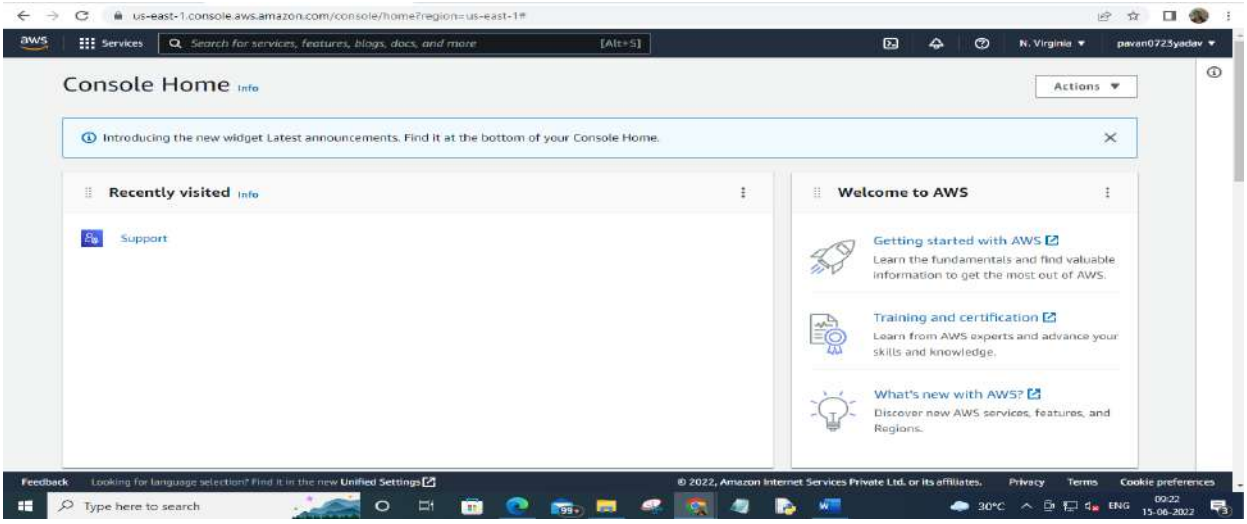


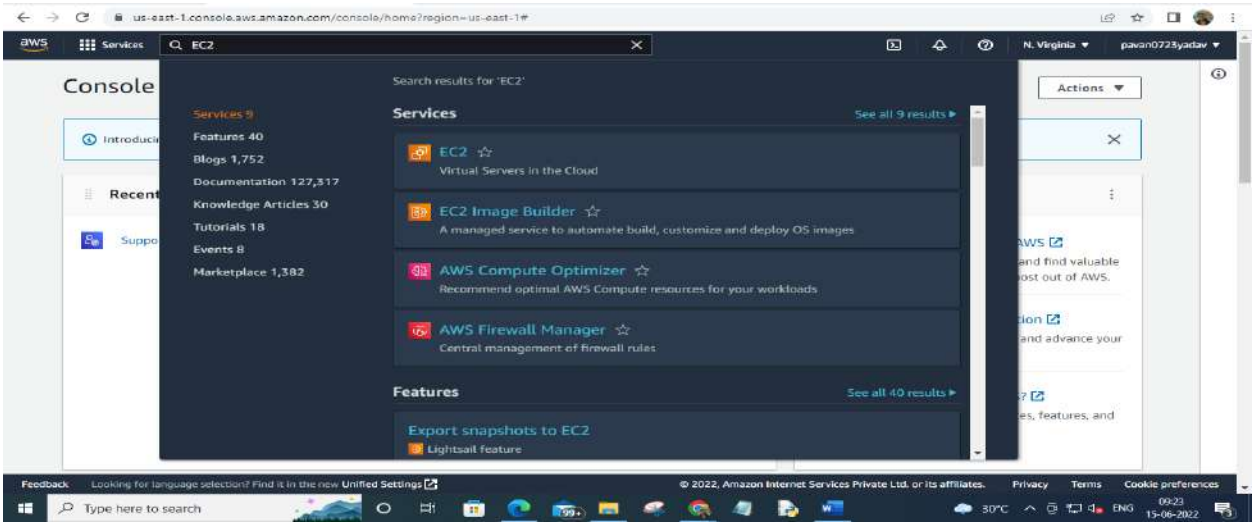


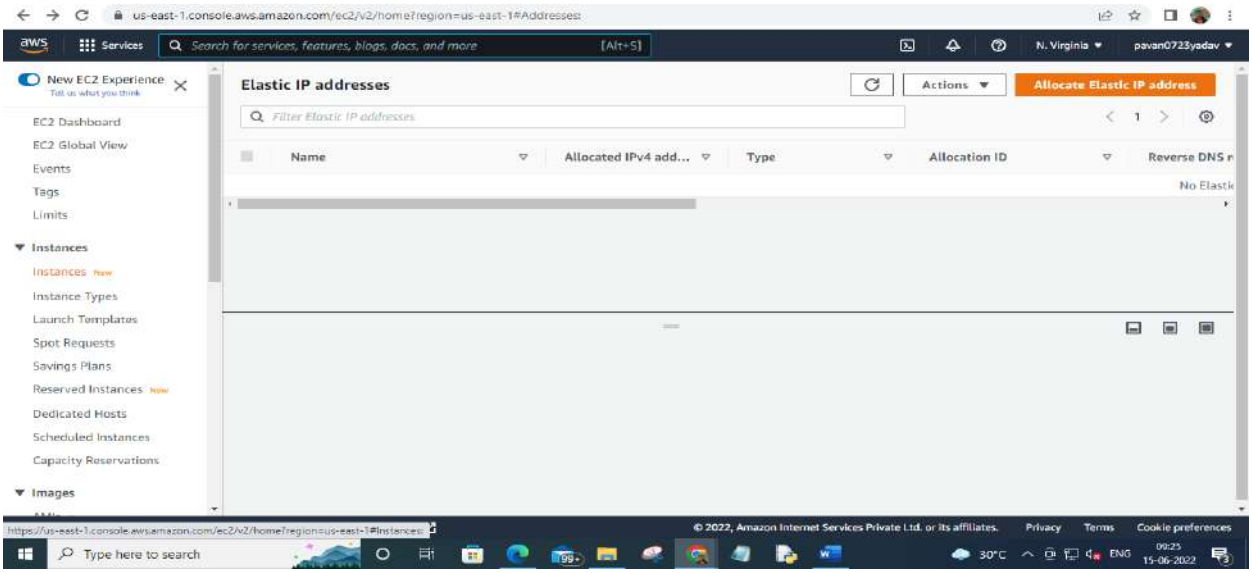


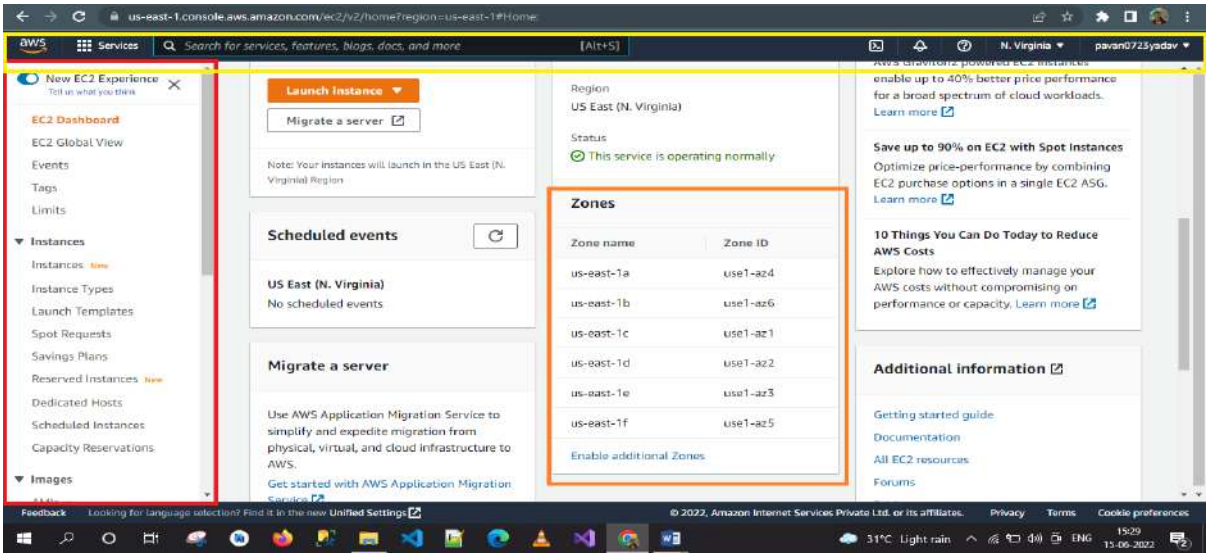
If you have reached this far, you have successfully finished Creating an AWS Account. Understand the AWS Free Tier The great thing about Amazon Web Services is that you get a free tier when you create an account. This is extremely useful if you want to learn AWS without spending money on provisioning servers and so on. However, not all stuff available on AWS qualifies for Free. Also, there are categories such as Always Free and 12 Months Free. You can get more details about them at this link.

B] Getting Familiarized with the AWS Console









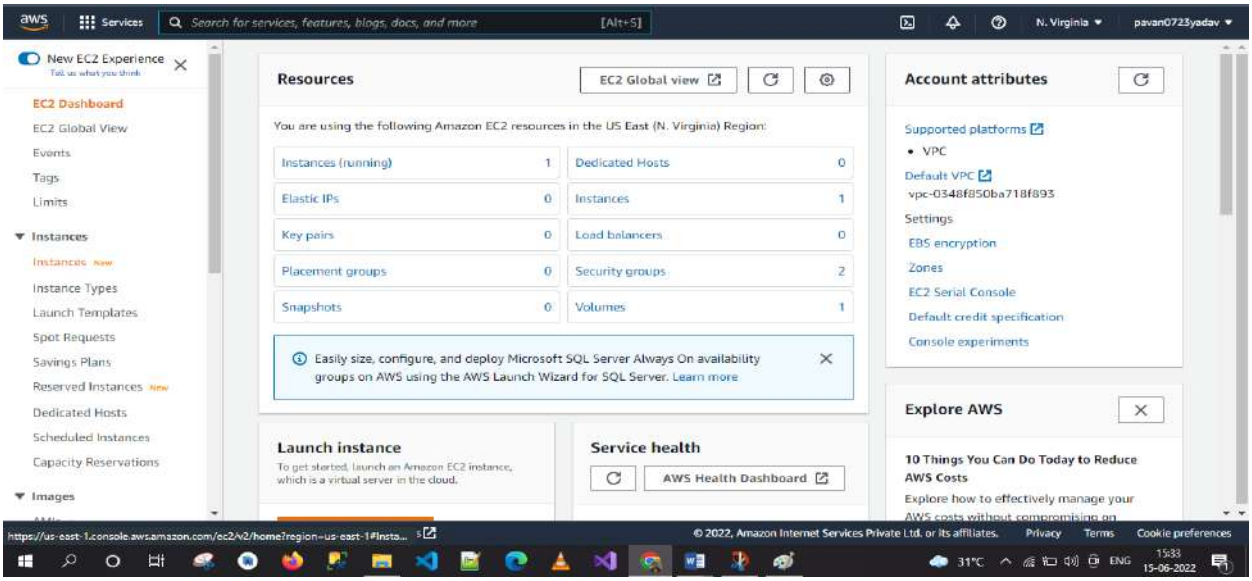
Navigation Bar

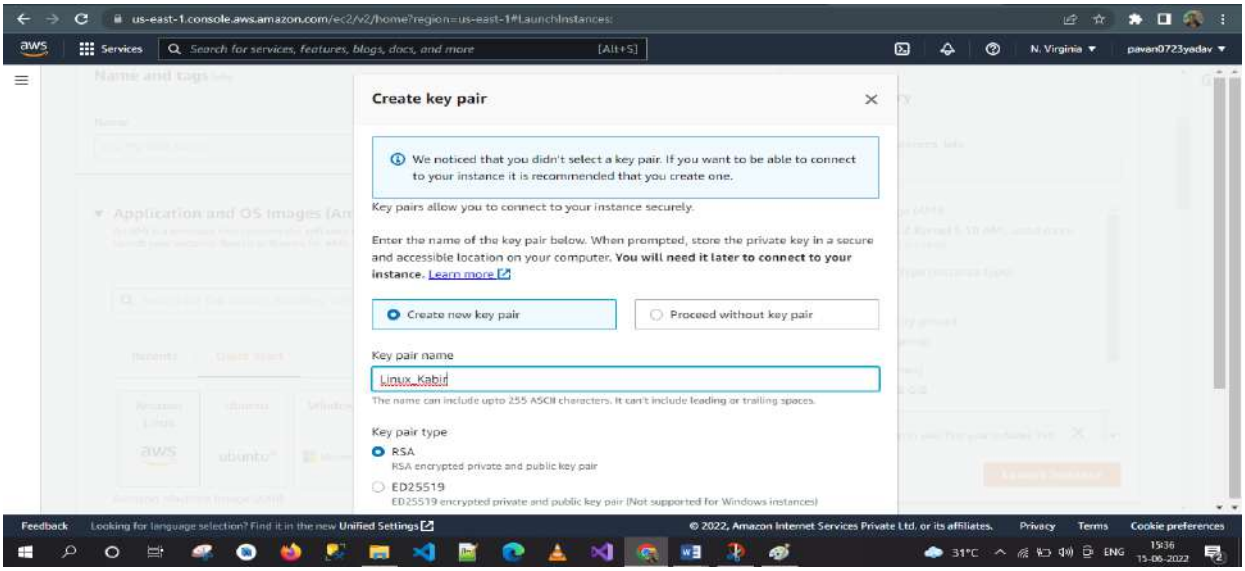
Navigation Pane

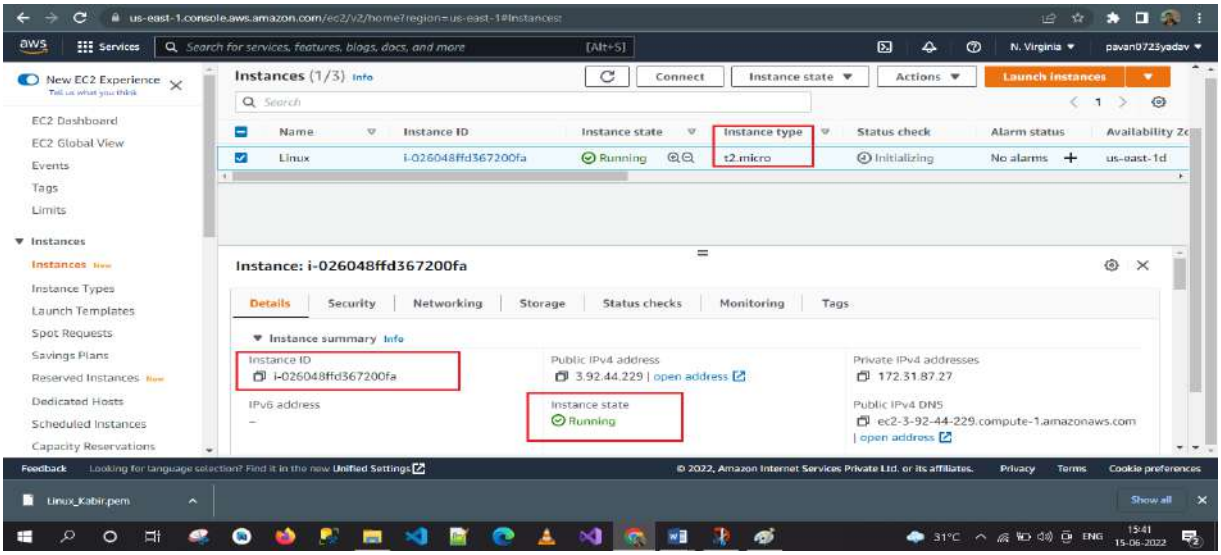
Select instance

Zones

Region







1 Instance ID

Instances provide a balance of compute, memory and networking resources, and can be used for a variety of diverse workloads. These instances are ideal for applications that use these resources in equal proportions such as web servers and code repositories.

Your Amazon Connect instance ID is the 36-character string at the end of your instance's Amazon Resource Name (ARN). To see your instance's ARN, follow the instructions in Find your Amazon Connect instance ID/ARN.

2 Instance Status

With instance status monitoring, you can quickly determine whether Amazon EC2 has detected any problems that might prevent your instances from running applications Status checks are performed every minute, returning a pass or a fail status. If all checks pass, the overall status of the instance is OK.

There are two types of status checks: system status checks and instance status checks.

System status checks

System status checks monitor the AWS systems on which your instance runs. These checks detect underlying problems with your instance that require AWS involvement to repair.

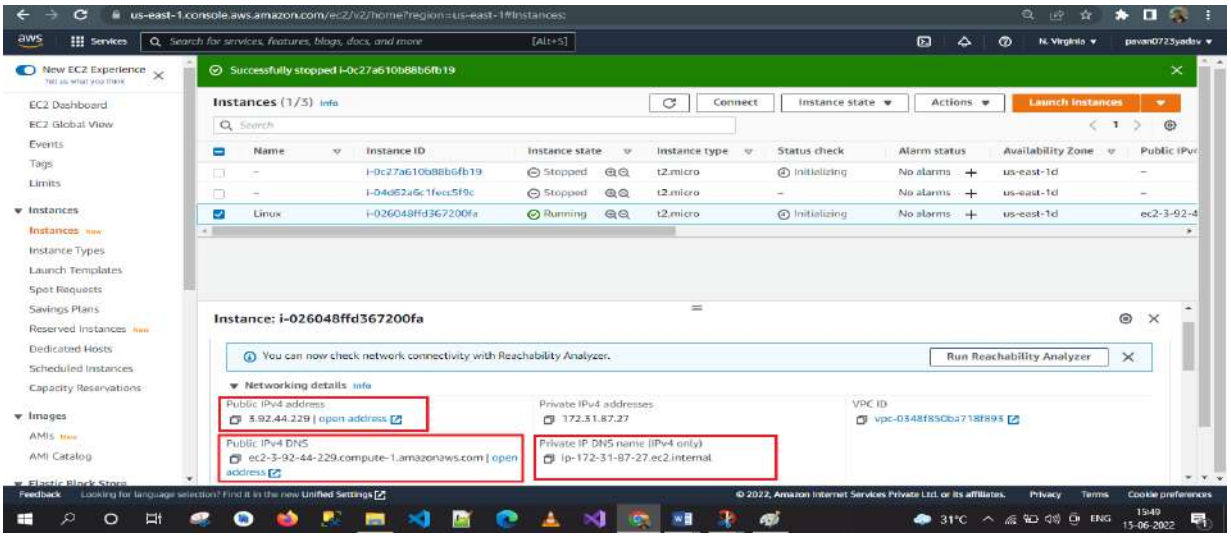
Instance status checks

Instance status checks monitor the software and network configuration of your individual instance. Amazon EC2 checks the health of the instance by sending an address resolution protocol (ARP) request to the network interface (NIC).

3 Instance Type

Amazon EC2 provides a wide selection of instance types optimized for different use cases. To determine which instance types meet your requirements, such as supported Regions, compute resources, or storage resources, see Find an Amazon EC2 instance type.

Go to the **Networking** Tab



Public DNS

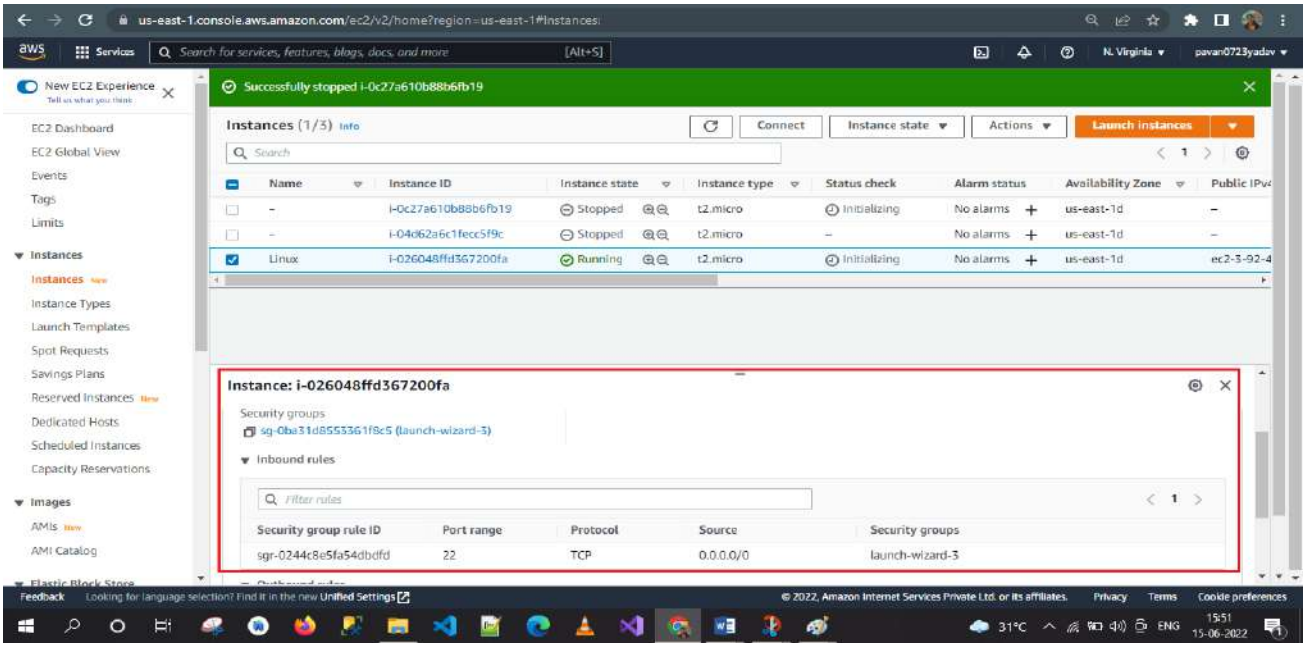
Dynamic DNS services provide custom DNS host names within their domain area that can be easy to remember and that can also be more relevant to your host's use case; some of these services are also free of charge. You can use a dynamic DNS provider with Amazon EC2 and configure the instance to update the IP address associated with a public DNS name each time the instance starts.

Private IP's

A private IPv4 address is an IP address that's not reachable over the Internet. You can use private IPv4 addresses for communication between instances in the same VPC.

A private IPv4 address, regardless of whether it is a primary or secondary address, remains associated with the network interface when the instance is stopped and started, or hibernated and started, and is released when the instance is terminated.

Go to **Security** Tab



Practical 2: An AWS IAM User: Creating an AWS IAM User.

A. Explore users and groups.
B. Add users to groups
C. Sign-In and test the users

Aim

1. Exploring pre-created IAM Users and Groups
2. Inspecting IAM policies as applied to the pre-created groups
3. Following a real-world scenario, adding users to groups with specific capabilities enabled
4. Locating and using the IAM sign-in URL
5. Experimenting with the effects of policies on service access

AWS Identity and Access Management

AWS Identity and Access Management (IAM) is a web service that enables Amazon Web Services (AWS) customers to manage users and user permissions in AWS. With IAM, you can centrally manage users, security credentials such as access keys, and permissions that control which AWS resources users can access.

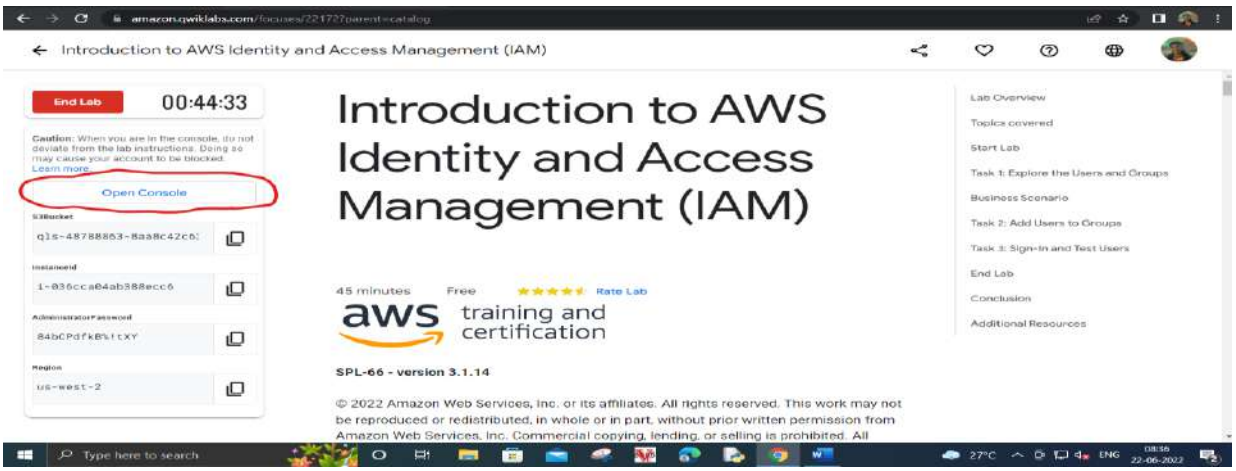
AWS Identity and Access Management (IAM) can be used to:

1. Manage IAM Users and their access: You can create Users and assign them individual security credentials (access keys, passwords, and multi-factor authentication devices). You can manage permissions to control which operations a User can perform.
2. Manage IAM Roles and their permissions: An |AM Role is similar to a User; in that it is an AWS identity with permission policies that determine what the - identity can and cannot do in AWS. However, instead of being uniquely associated with one person, a Role is intended to be assumable by anyone who needs it.
3. Manage federated users and their permissions: You can enable identity federation to allow existing users in your enterprise to access the AWS Management Console, to call AWS APIs and to access resources, without the need to create an IAM User for each identity.

Task 1: Explore the Users and Groups

In this task, you will explore the Users and Groups that have already been created for you in IAM.

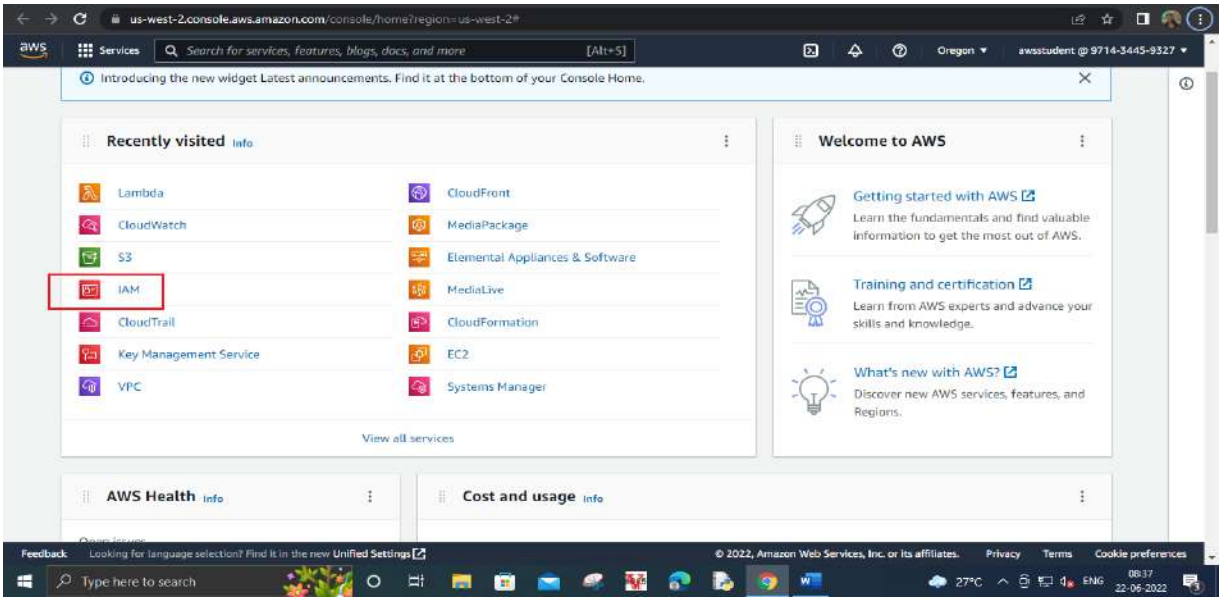
Step 1 – Start Lab and Open Console



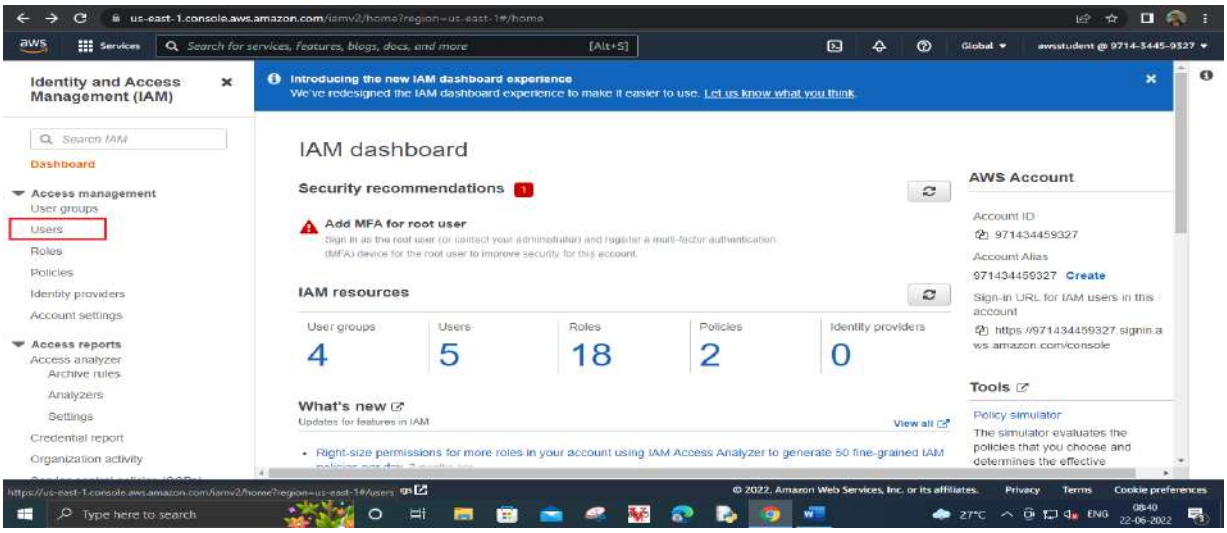
Step 2 – If you see the message, you must log out before logging into different AWS account to,

click here Click on here (hyperlink) to logout.

Step 3 – In the AWS Management Console, on the Services menu, click IAM.

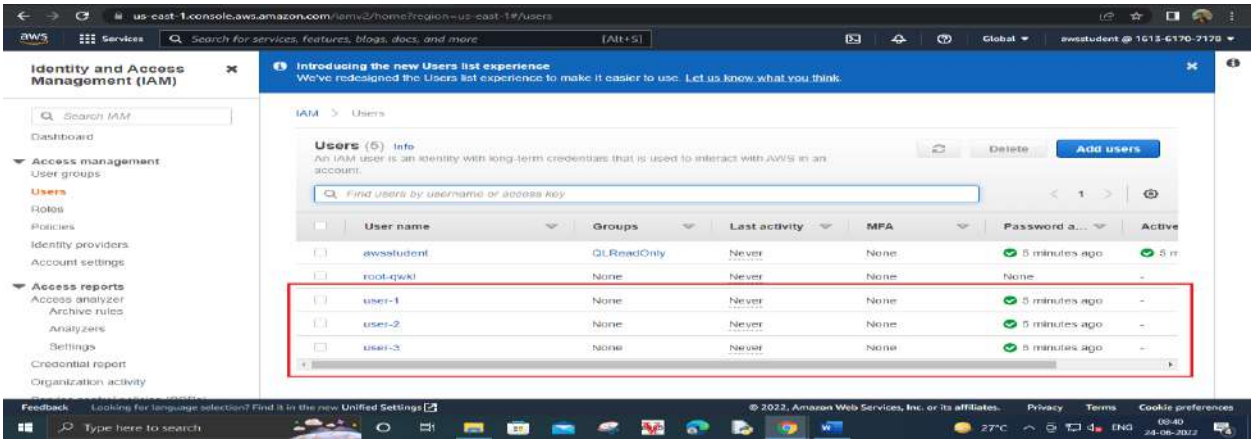


Step 4 – In the navigation pane on the left, click Users.

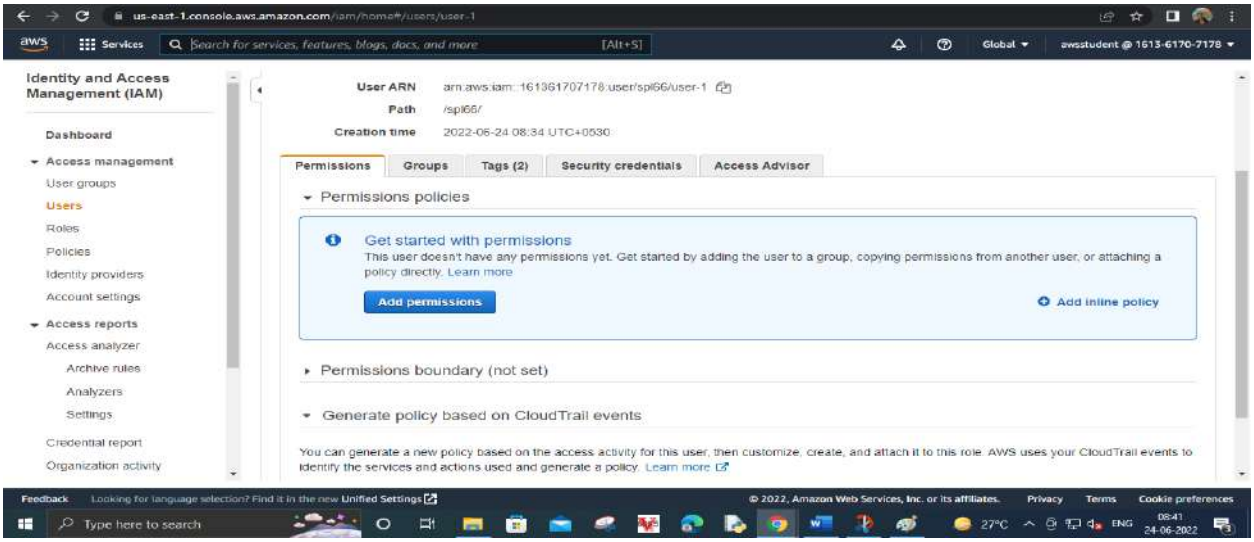


Step 5 – The following IAM Users have been created for you:

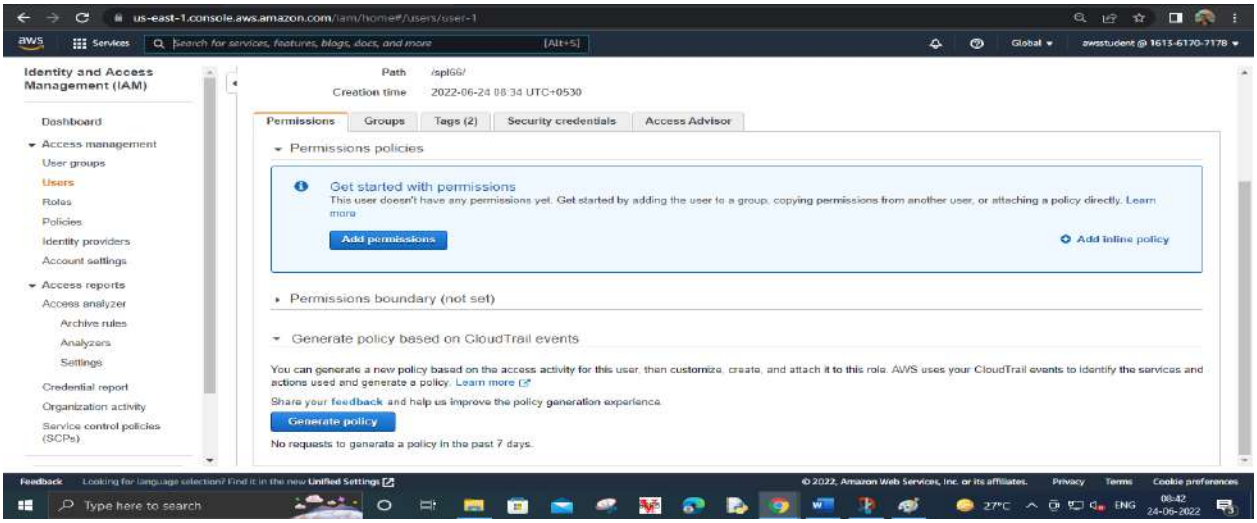
- user-1
- user-2
- User-3



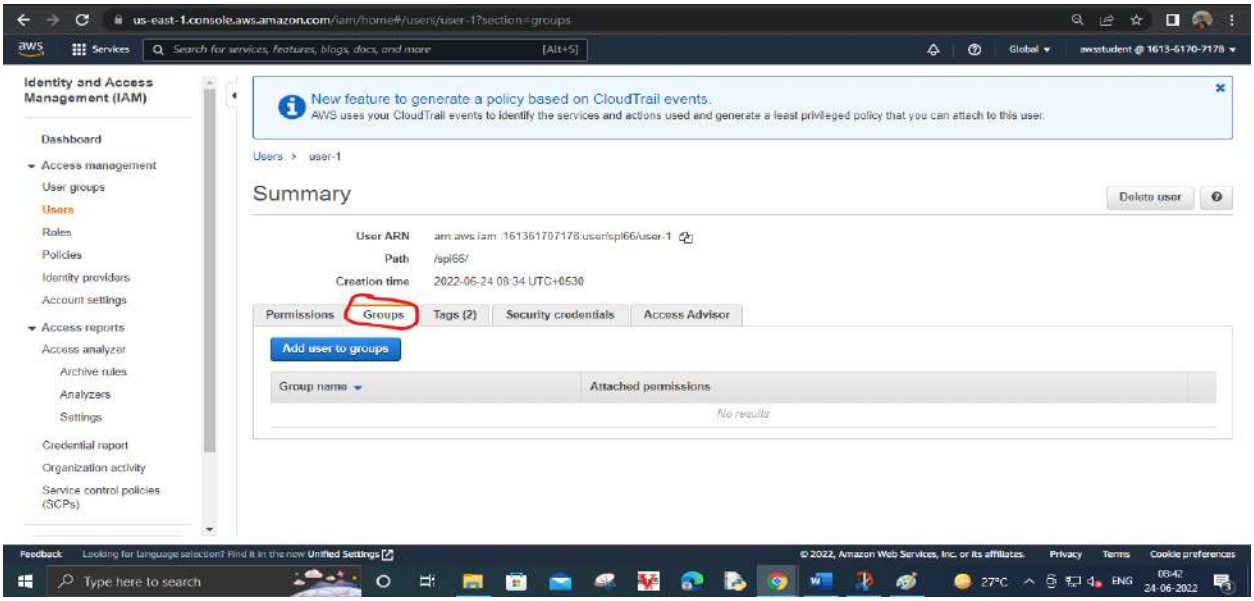
Step 6 – Click user-1. This will bring to a summary page for user-displayed.



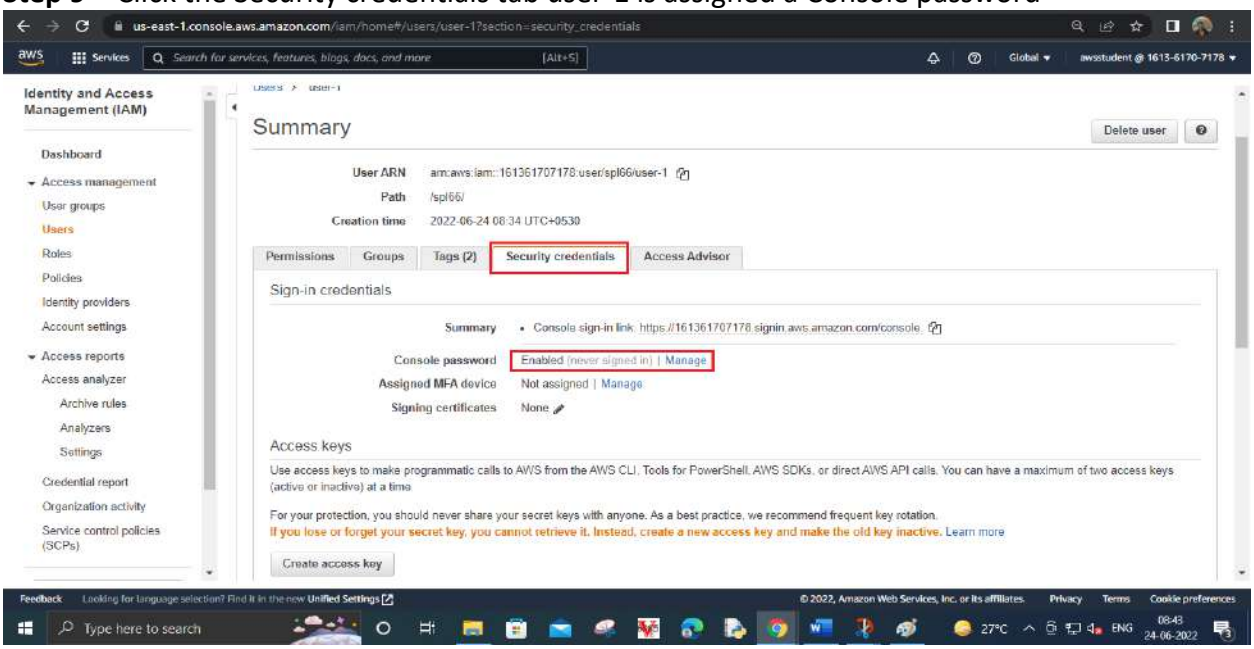
Step 7 – Notice that user-1 does not have any permissions.



Step 8 – Click the Groups tab.user-1 also is not a member of any groups.

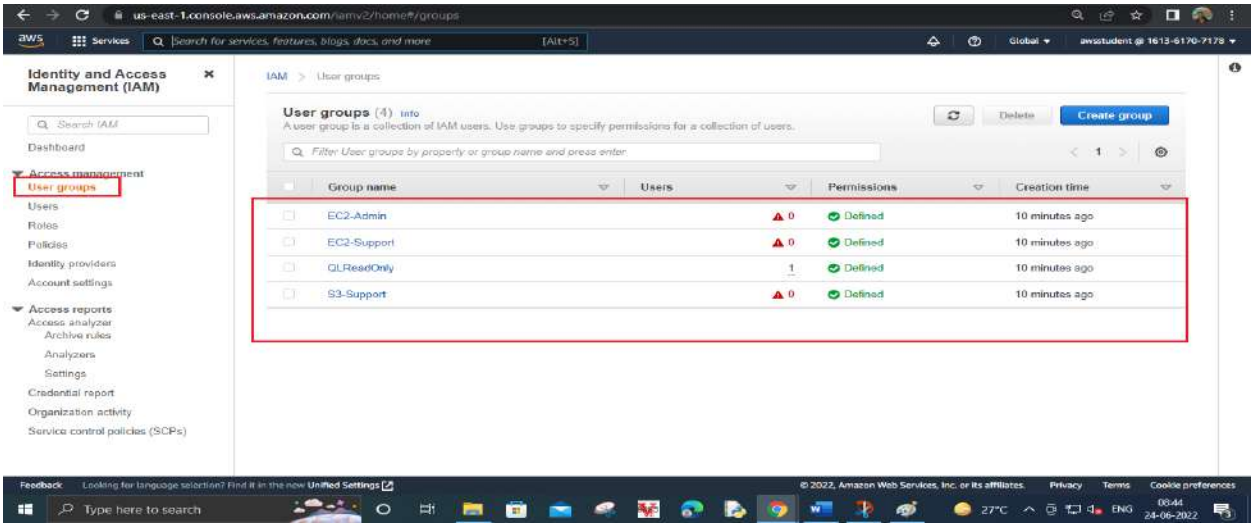


Step 9 – Click the Security credentials tab user-1 is assigned a Console password

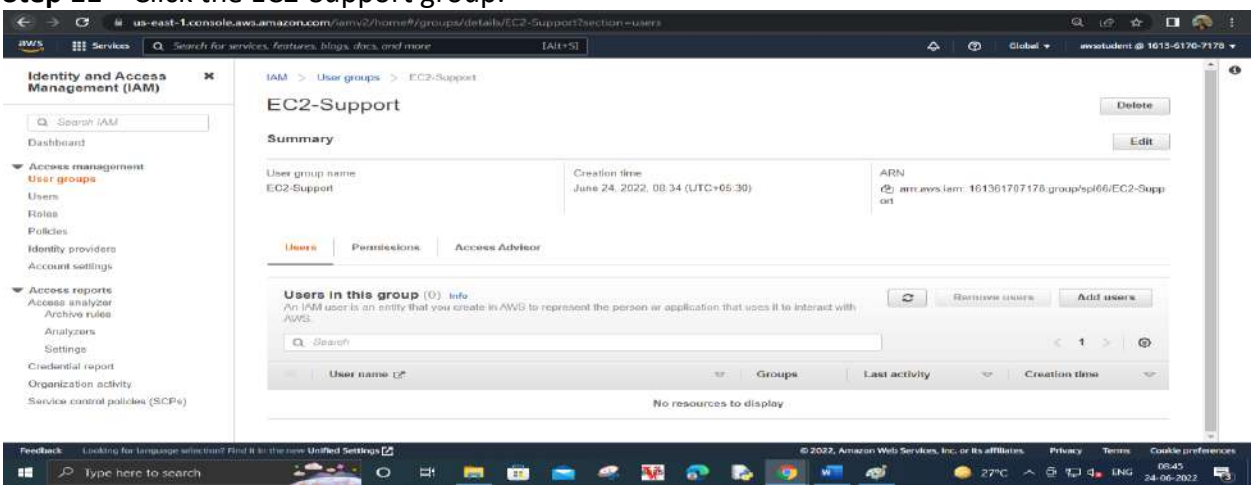


Step 10 – In the navigation pane on the left, click Groups.
The following groups have already been created for you:

1. EC2-Admin
2. EC2-Support
3. S3-Support

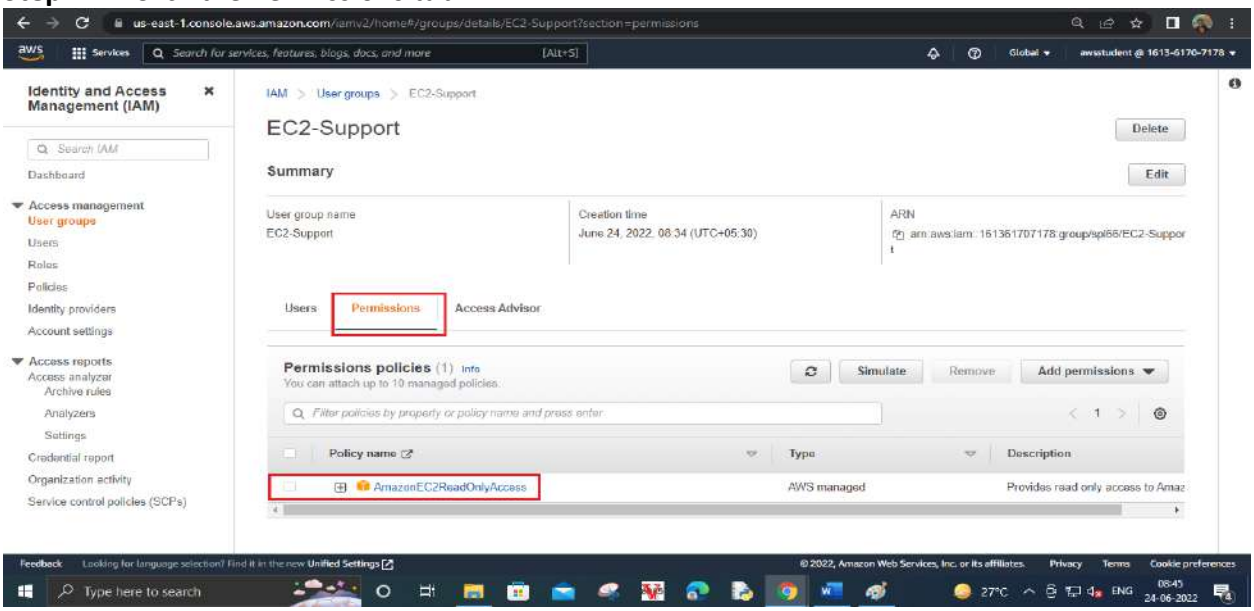


Step 11 – Click the EC2-Support group.



This will bring you to the summary page for the EC2-Support group.

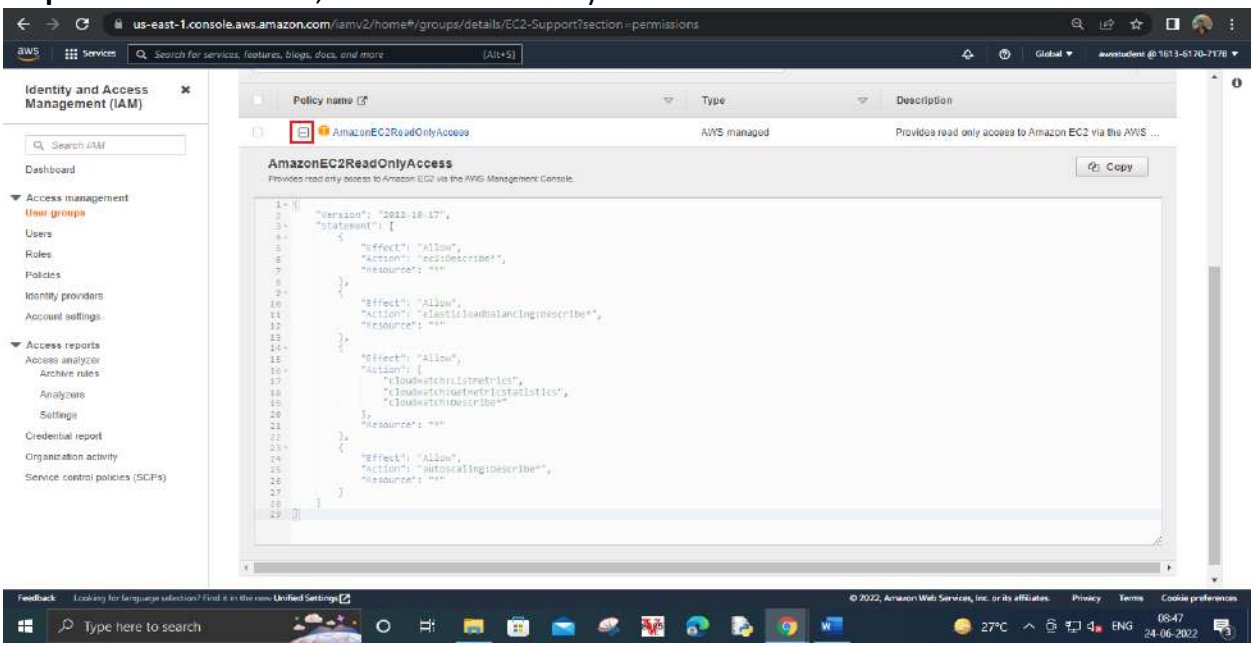
Step 12 – Click the Permissions tab.



This group has a Managed Policy associated with it, calledAmazonEC2ReadOnlyAccess. Managed Policies are pre-built policies (built either by AWS or by your administrators) that can be attached to IAM Users and Groups.

When the policy is updated, the changes to the policy are immediately apply against all Users and Groups that are attached to the policy.

Step 13 – Under Actions, click the Show Policy link.



A policy defines what actions are allowed or denied for specific AWS resources. This policy is granting permission to List and Describe information about EC2, ElasticLoad Balancing, CloudWatch and Auto Scaling. This ability to view 'resources, but not modify them, is ideal for assigning to a Support role. The basic structure of the statements in an IAM Policy is:

1. Effect says whether to Allow or Deny the permissions.

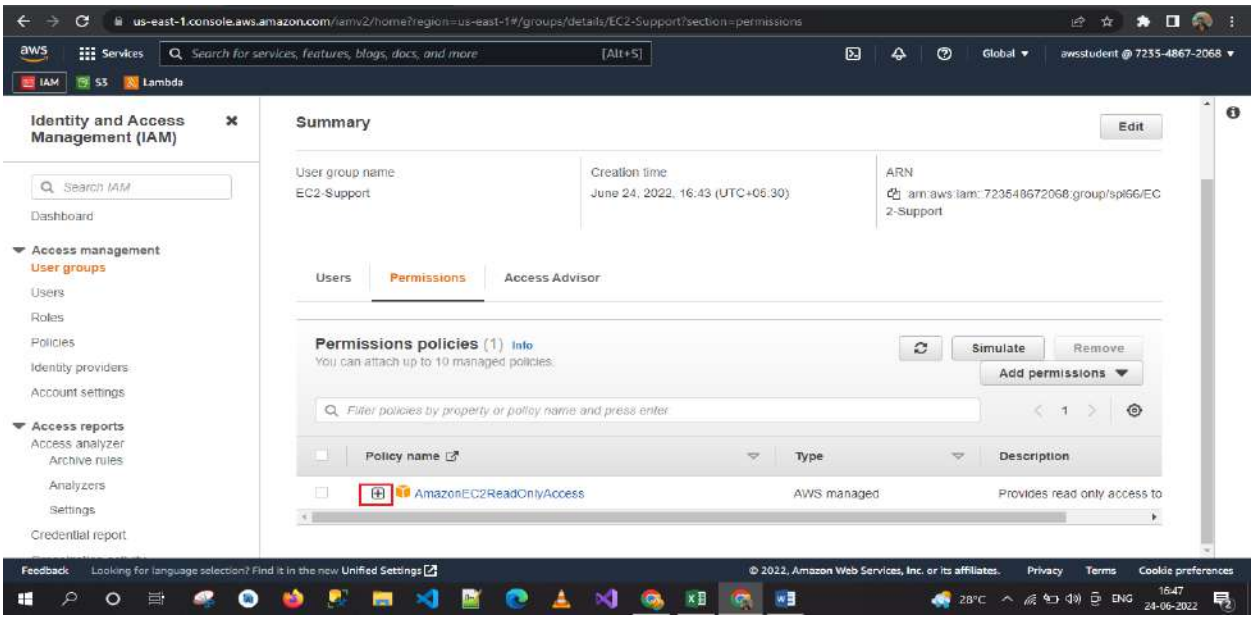
2. Action specifies the API calls that can be made against an AWS Service (e.g. cloudwatch:ListMetrics).

3. Resource defines the scope of entities covered by the policy rule (e.g. a specific Amazon S3 bucket or Amazon EC2 instance, or * which means any resource).

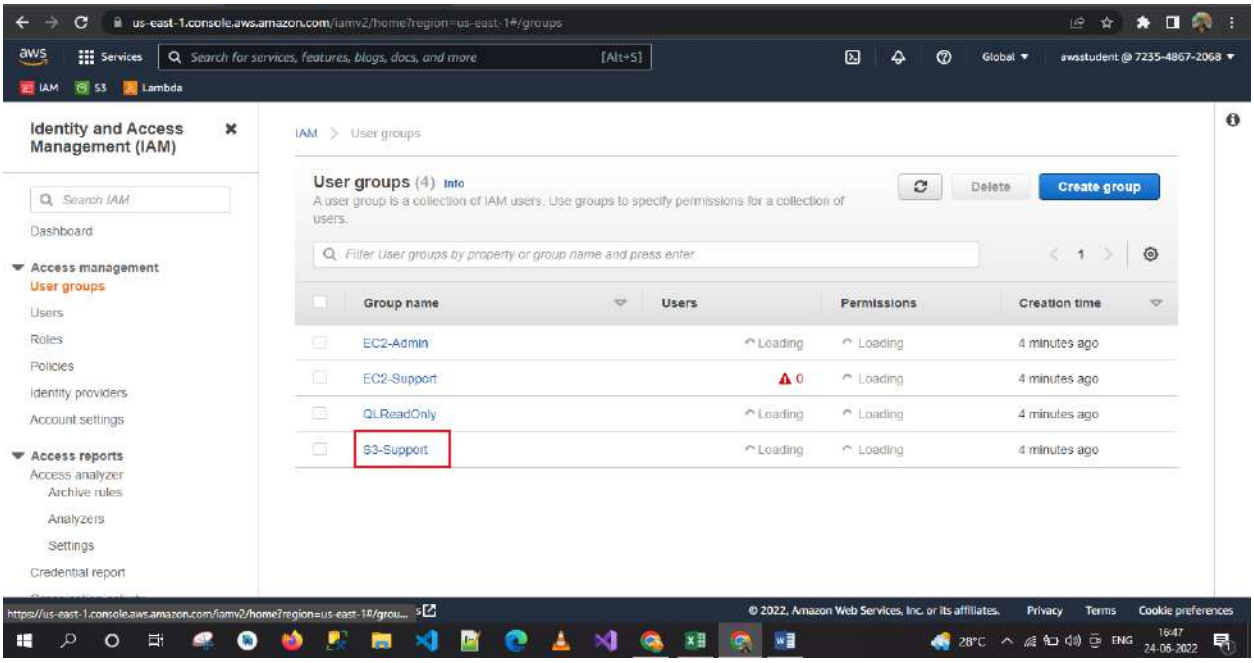
```
{
    "Effect": "Allow",
    "Action": "elasticloadbalancing:Describe*",
    "Resource": "*"
},
```

Step 13 – Close the Show Policy window.

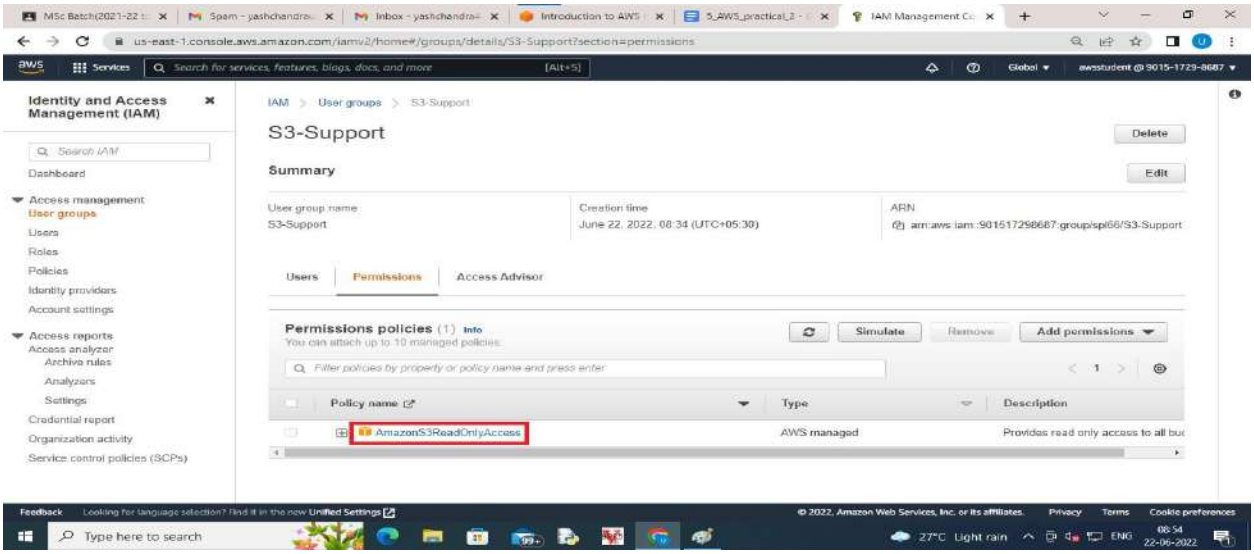
Step 14 – In the navigation pane on the left, click Groups.



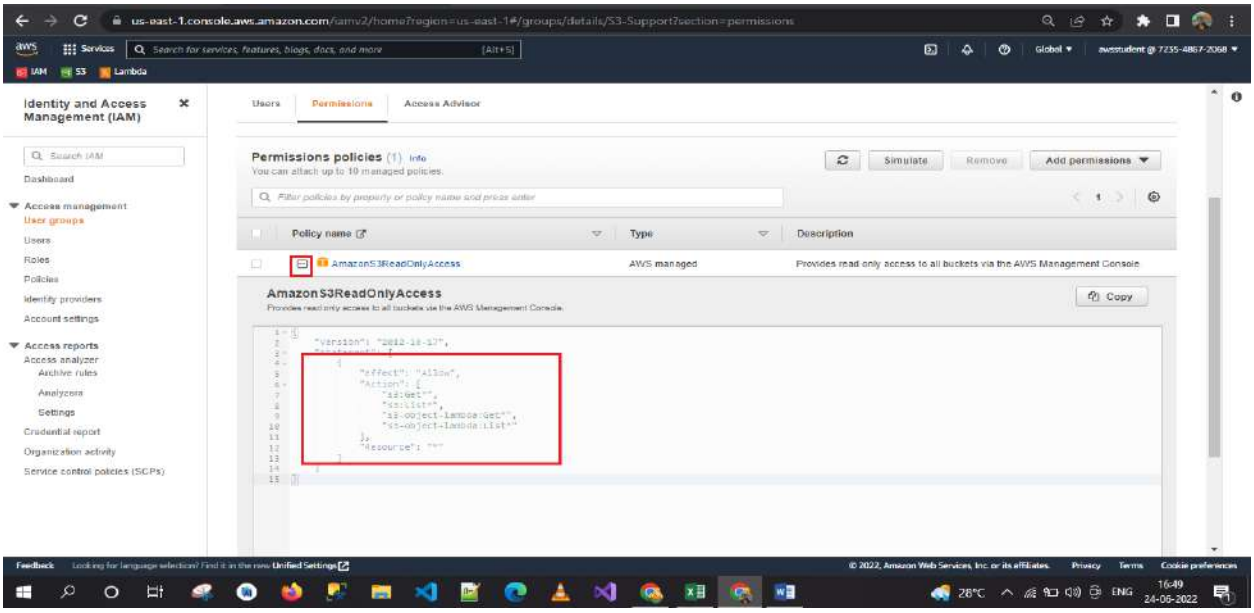
Step 15 – Click the S3-Support Group.



The S3-Support group has the AmazonS3ReadOnlyAccess policy attached.

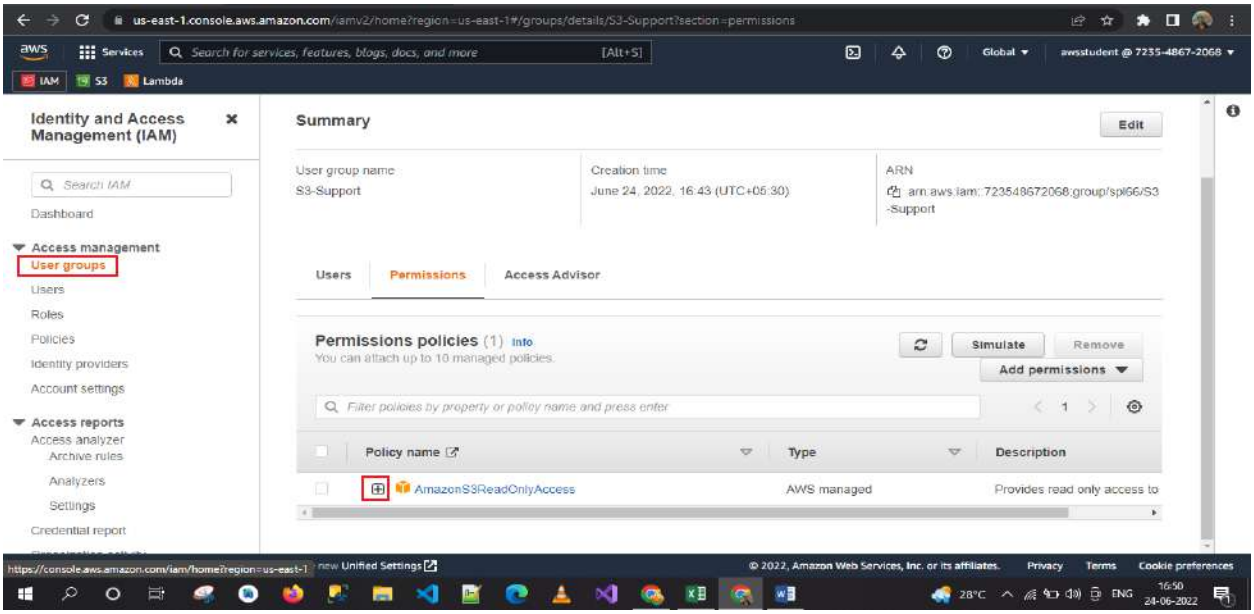


Step 16 – Below the Actions menu, click the Show Policy link. This policy has permissions to Get and List resources in Amazon S3.

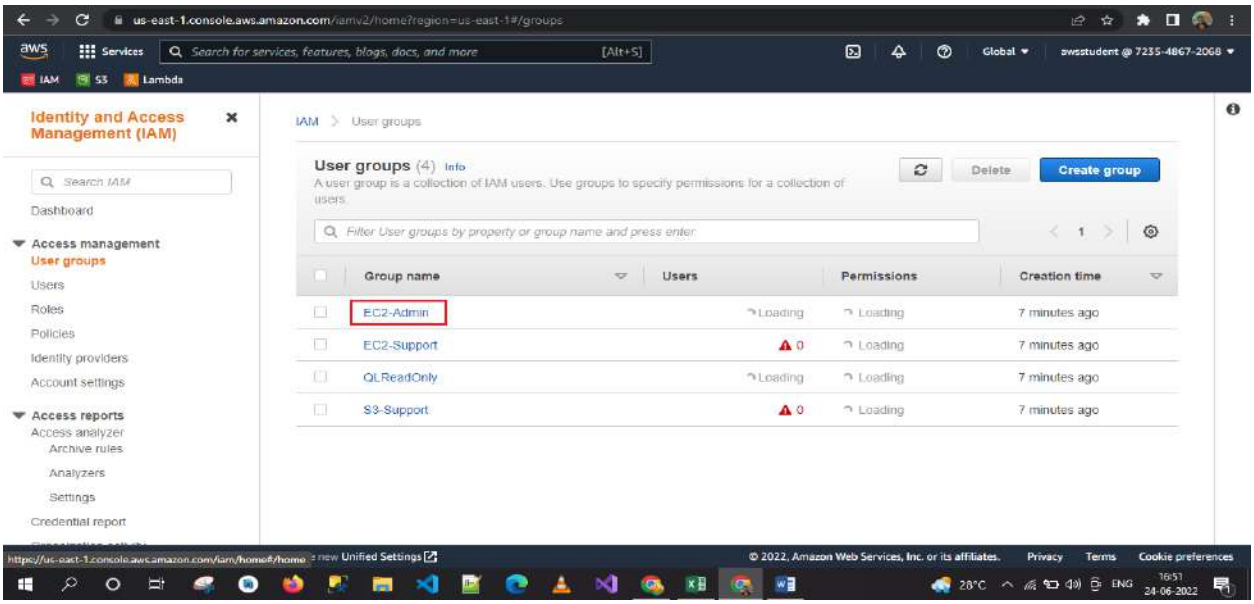


Step 17 – Close the Show Policy window.

Step 18 – In the navigation pane on the left, click Groups.

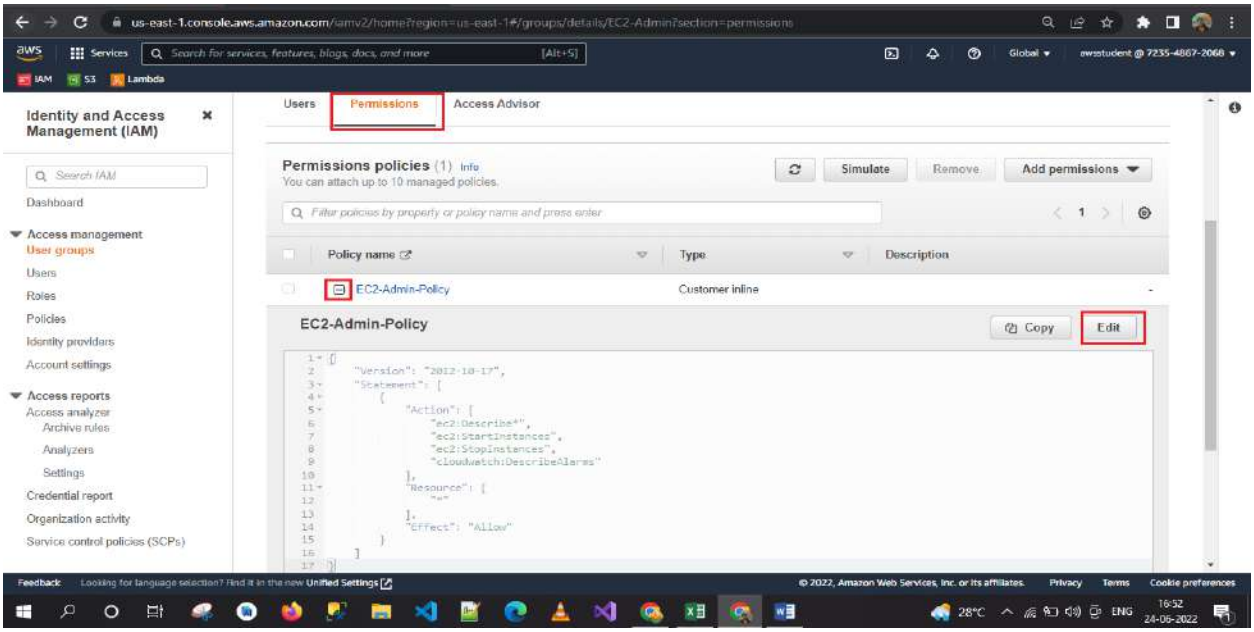


Step 19 – Click the EC2-Admin group



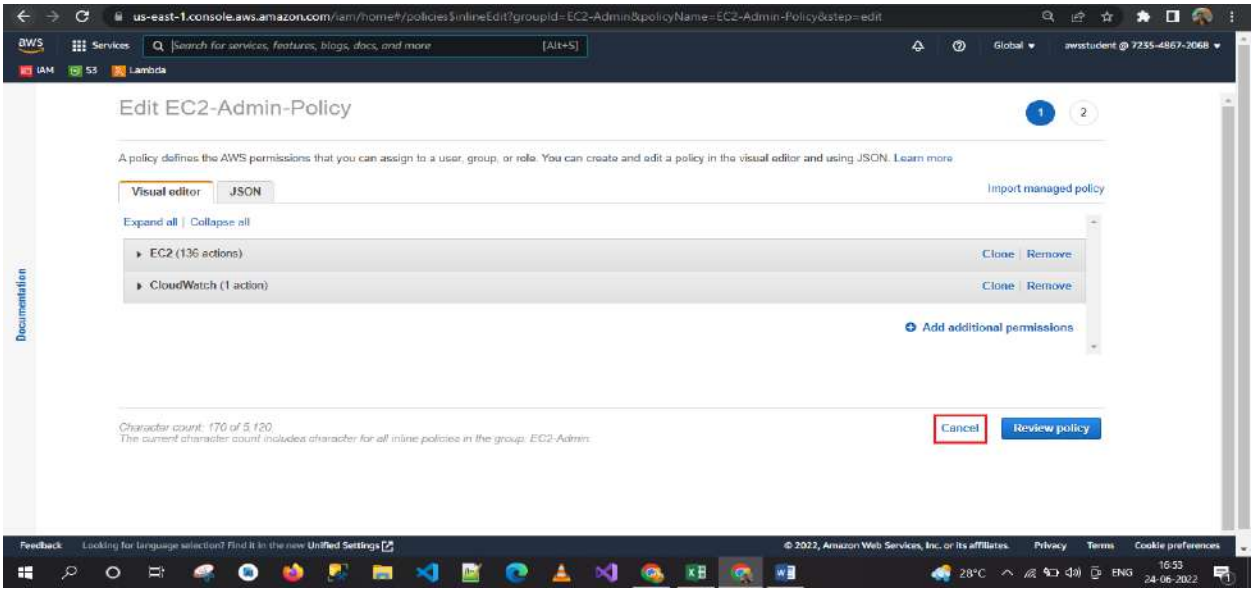
This Group is slightly different from the other two. Instead of a Managed Policy, it has anInline Policy, which a policy is assigned to just one User or Group. Inline Policies are typically used to apply permissions for one-off situations.

Step 20 – Under Actions, click Edit Policy to view the policy



This policy grants permission to view (Describe) information about Amazon EC2. And the ability to Start and Stop instances.

Step 21 – At the bottom of the screen, click Cancel to close the policy



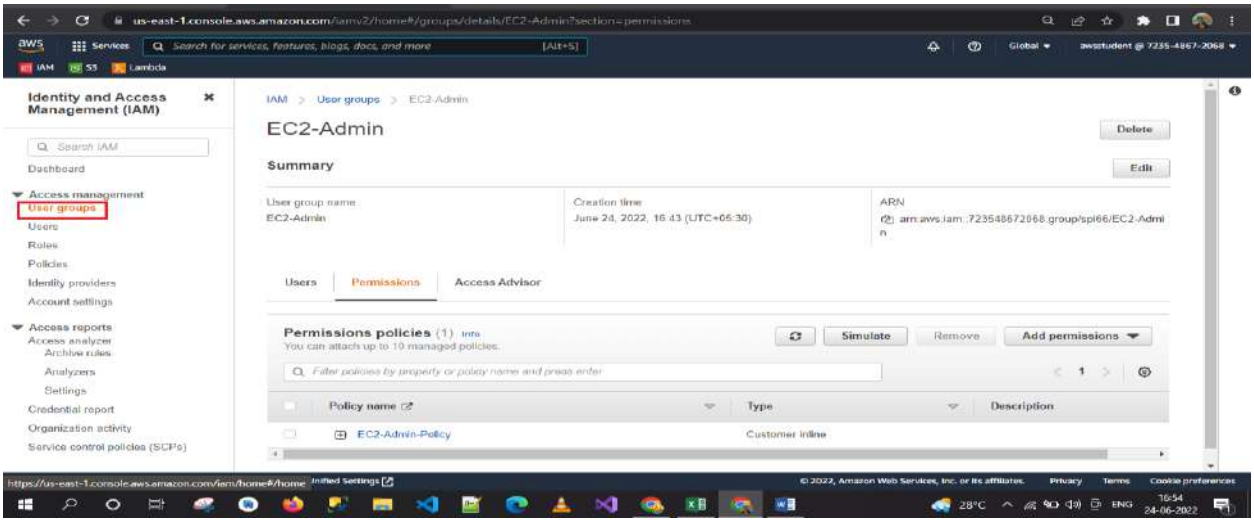
Business Scenario For the remainder of this lab, you will work with these Users and Groups to enable permissions supporting the following business scenario:

Your company is growing its use of Amazon Web Services, and is using many AmazonEC2 instances and a great deal of Amazon S3 storage. You wish to give access to new staff depending upon their job function: a. user-1 -> S3-Support Read-Only -> access to Amazon S3 b. user-2 -> EC2-Support Read-Only -> access to Amazon EC2 c. user-3 -> EC2-Admin -> View, Start and Stop Amazon EC2 instances

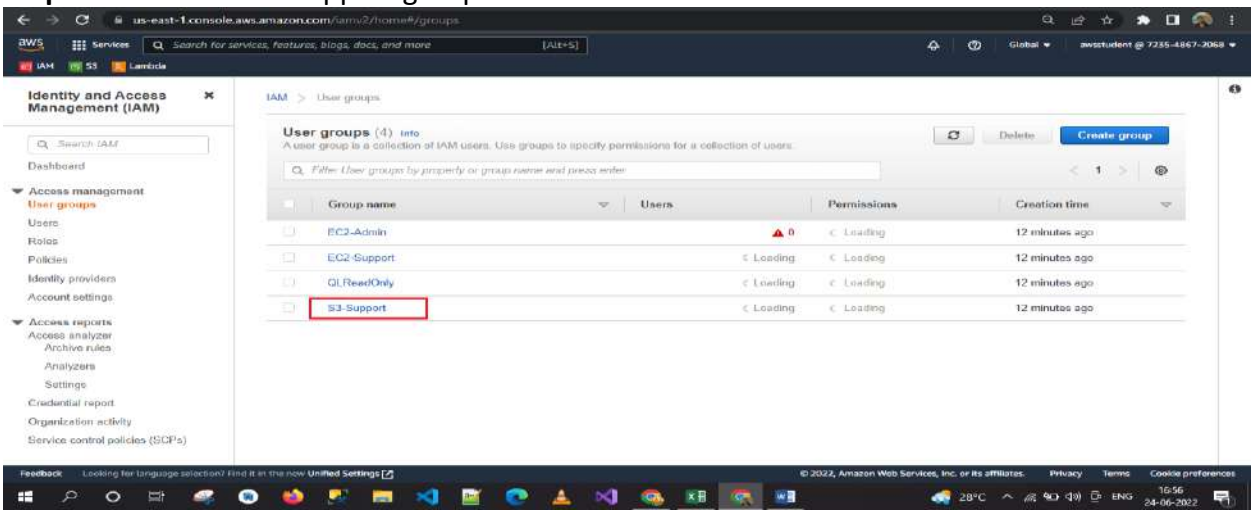
Task 2: Add Users to Groups

You have recently hired user-1 into a role where they will provide support for Amazon S3. You will add them to the S3-Support group so that they inherit the necessary permissions via the attached AmazonS3ReadOnlyAccess policy.

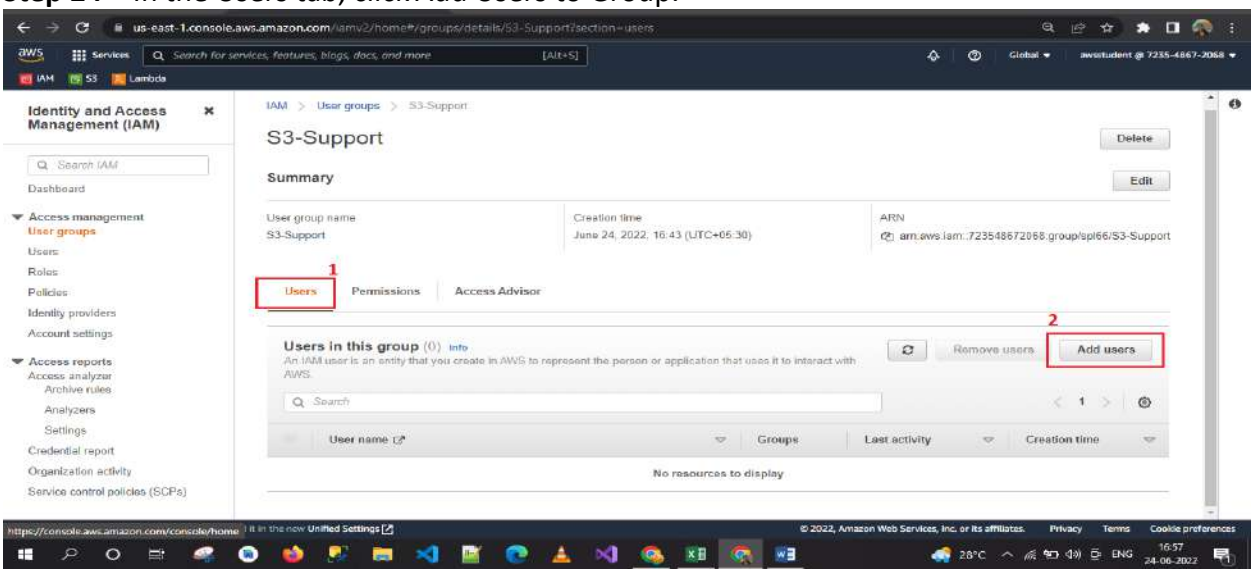
Step 22 – Add user-1 to the S3-Support Group In the left navigation pane, click Groups



Step 23 – Click the S3-Support group.

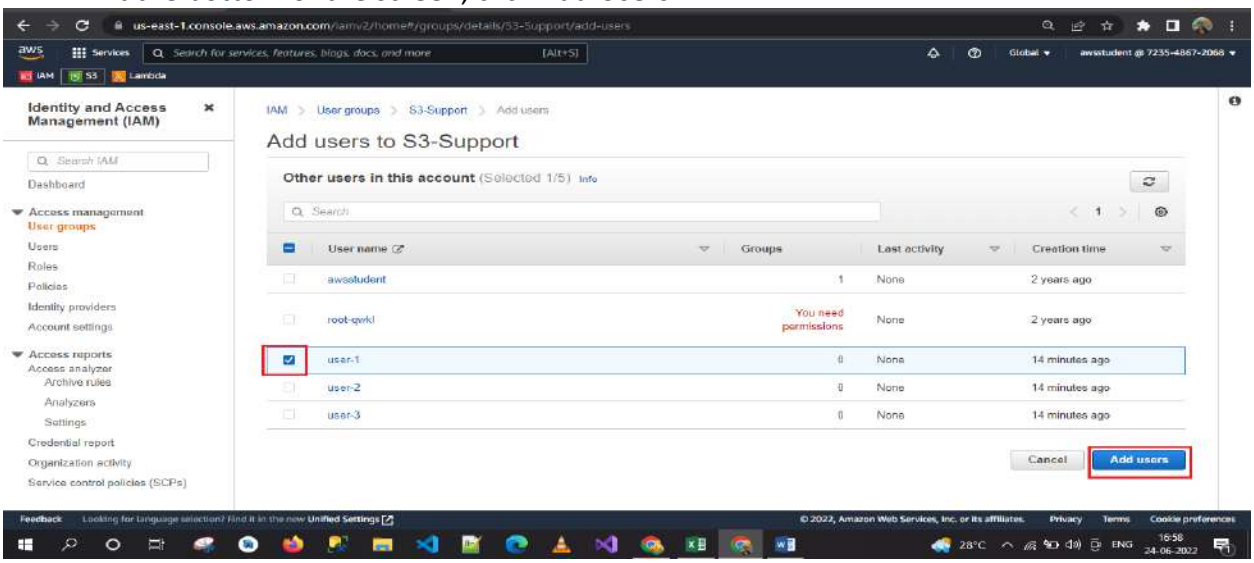


Step 24 – In the Users tab, click Add Users to Group.

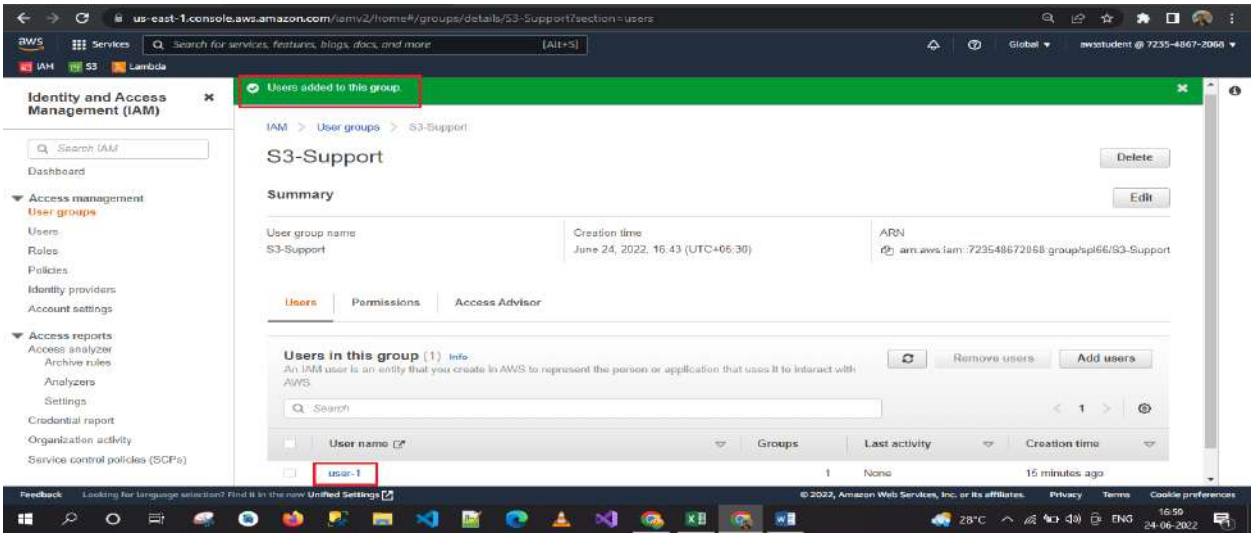


Step 25 – In the Add Users to Group window, configure the following:

1. Select user-1.
2. At the bottom of the screen, click Add Users.



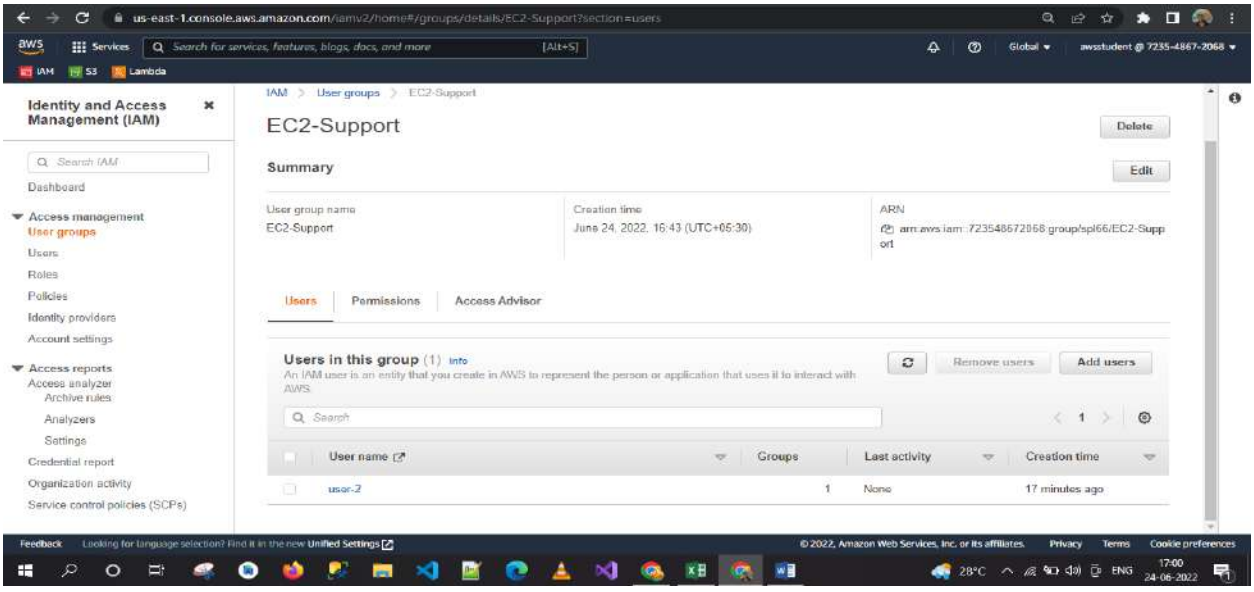
In the Users tab you will see that user-1 has been added to the group.



Add user-2 to the EC2-Support group

You have hired user-2 into a role where they will provide support for Amazon EC2.

Step 26 – Using similar steps to the ones above, add user-2 to the EC2-Support group. user-2 should now be part of the EC2 - Support group.

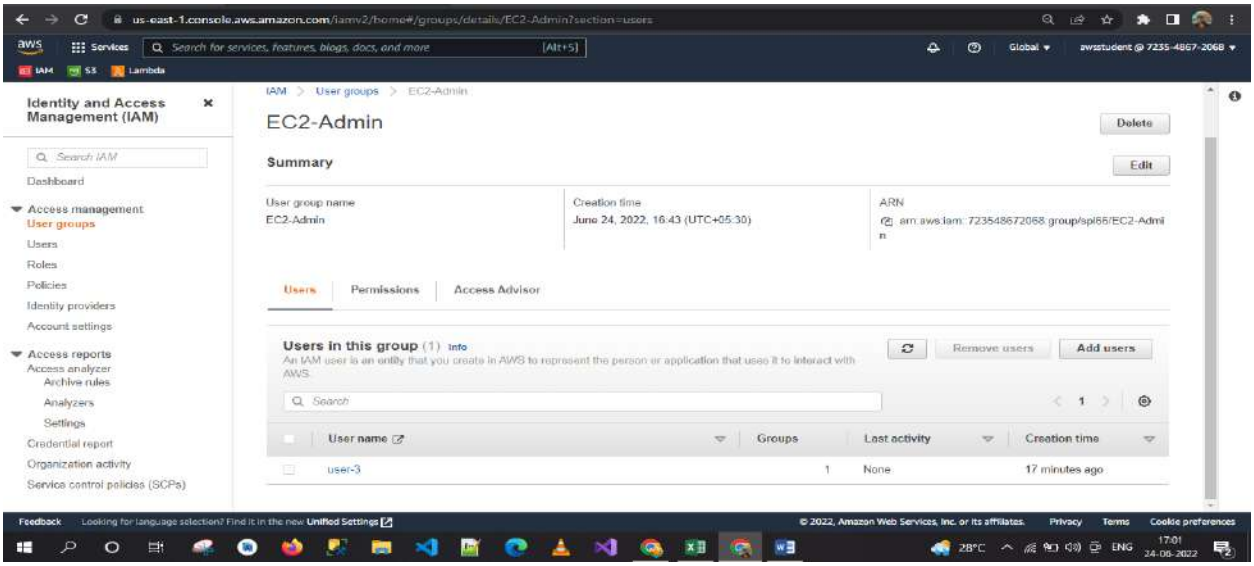


Add user-3 to the EC2-Admin Group.

You have hired user-3 as your Amazon EC2 administrator, who manage your EC2

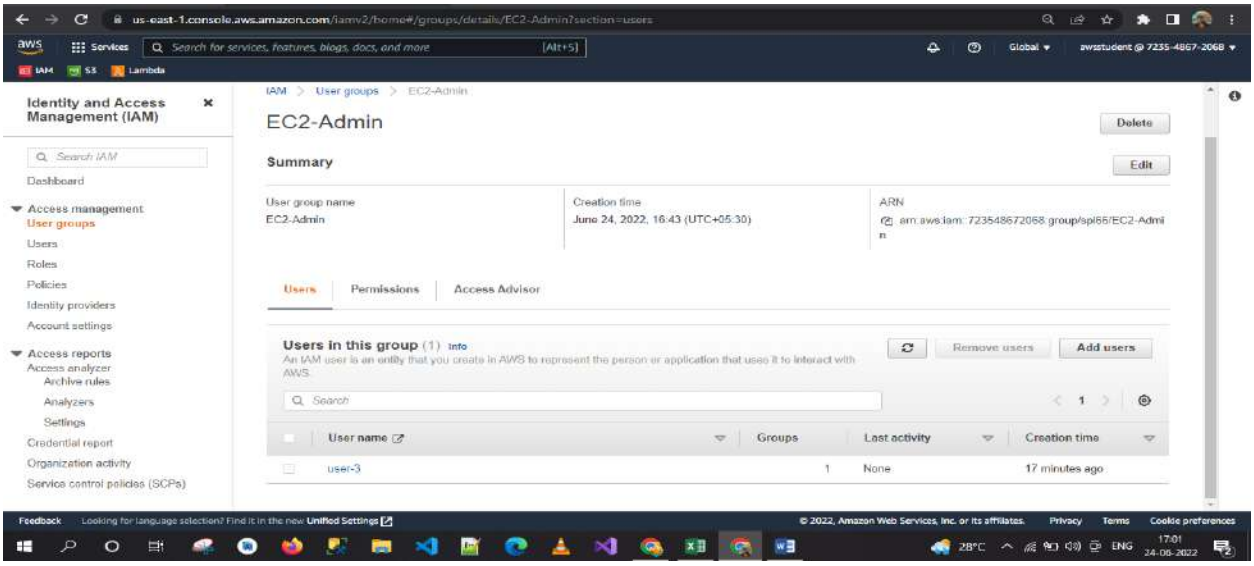
- instances.

Step 27 – Using similar steps to the ones above, add user-3 to the EC2-Admin group.
user-3 should now be part of the EC2-Admin group.

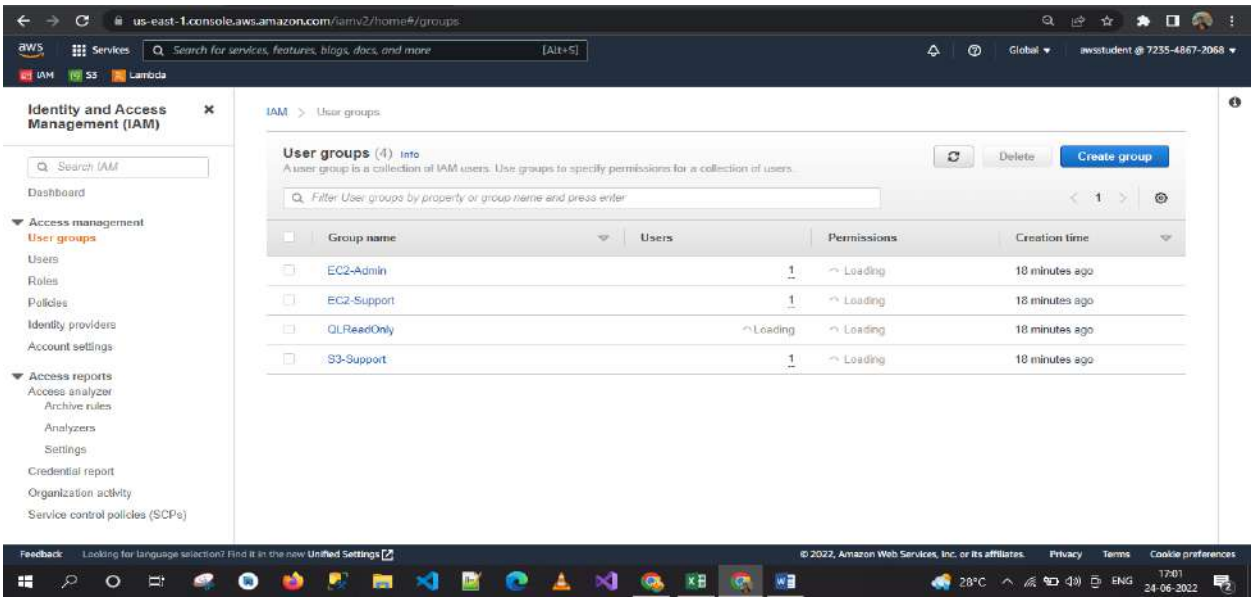


You have hired user-3 as your Amazon EC2 administrator, who manage your EC2 -instances.

Step 27 – Using similar steps to the ones above, add user-3 to the EC2-Admin group.
user-3 should now be part of the EC2-Admin group.



Step 28 – In the navigation pane on the left, click Groups.



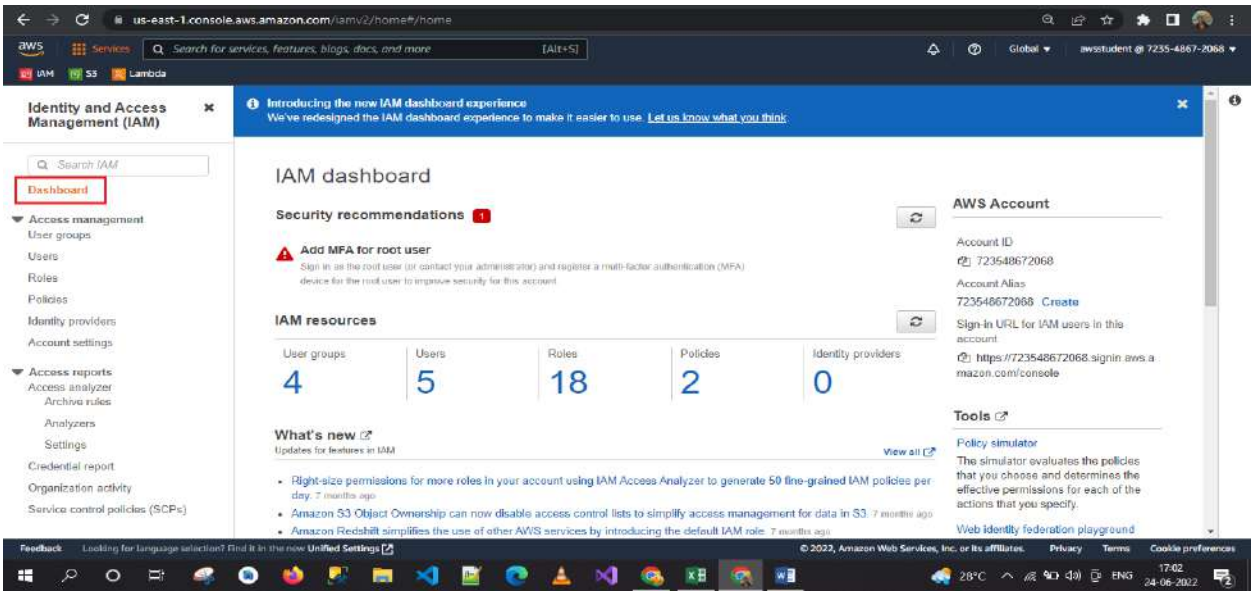
Each Group should have a 1 in the Users column for the number of Users in eachGroup.

If you do not have a 1 beside each group, revisit the above instructions above to ensure that each user is assigned to a Group, as shown in the table in the Business Scenario section.

Task 3: Sign-In and Test Users

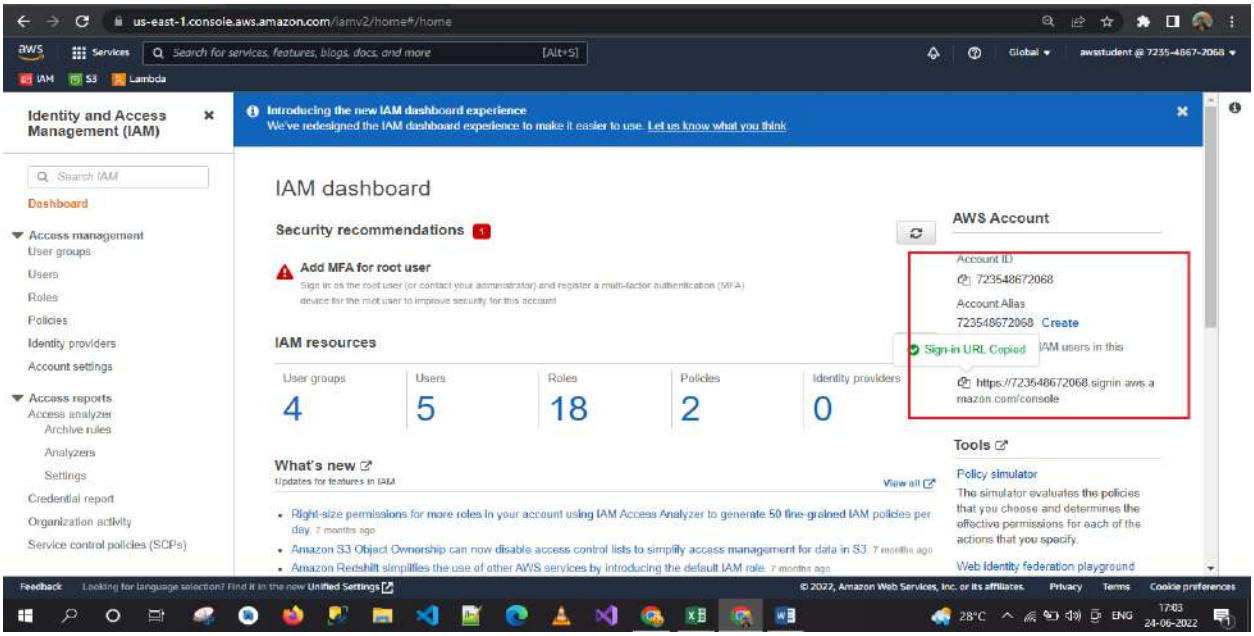
In this task, you will test the permissions of each IAM User.

Step 29 – In the navigation pane on the left, click Dashboard.



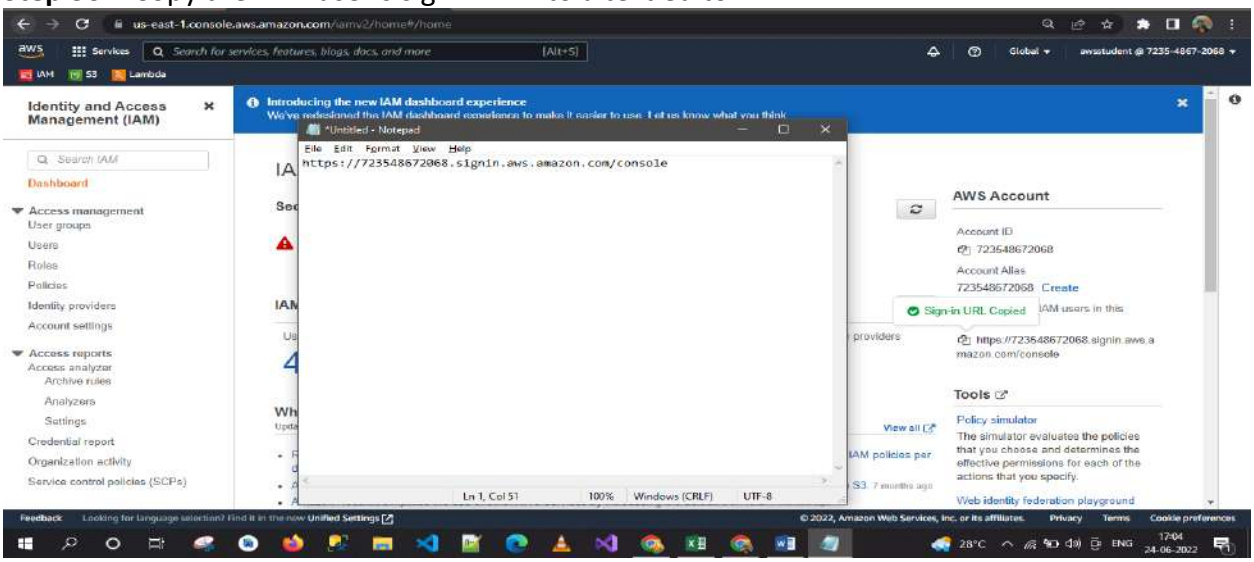
An IAM users sign-in link is displayed It will look similar to:

https://723548672068.signin.aws.amazon.com/console



This link can be used to sign-in in to the AWS Account you are currently using.

Step 30 – Copy the IAM user's sign-in link to a text editor.



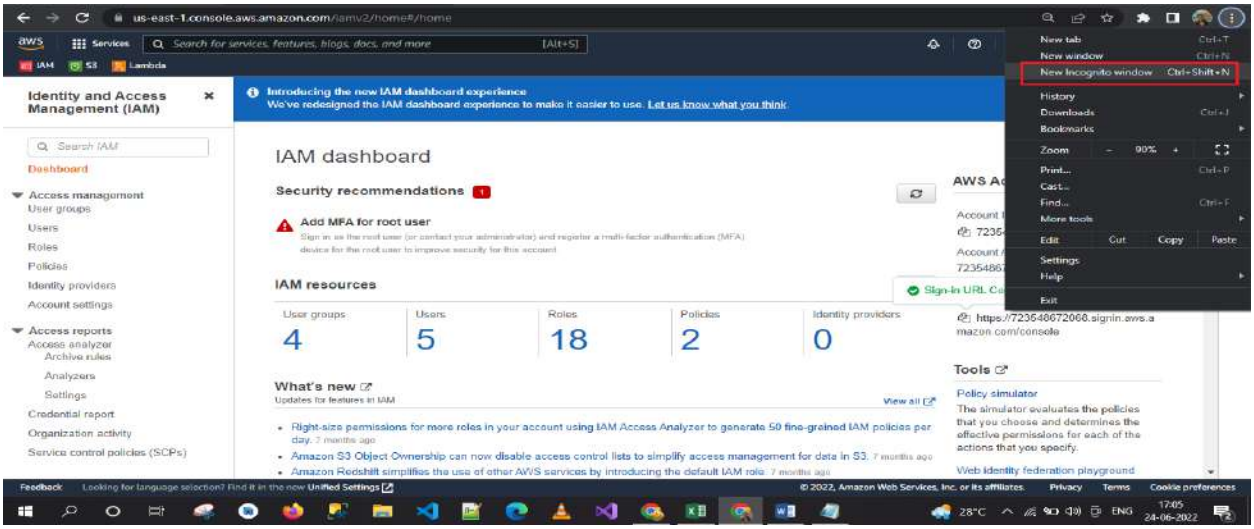
Step 31 – Open a private window.

Step 32 – Mozilla Firefox

- Click the menu bars at the top-right of the screen
- Select New Private Window

Google Chrome

- Click the ellipsis at the top-right of the screen
- Click New incognito window



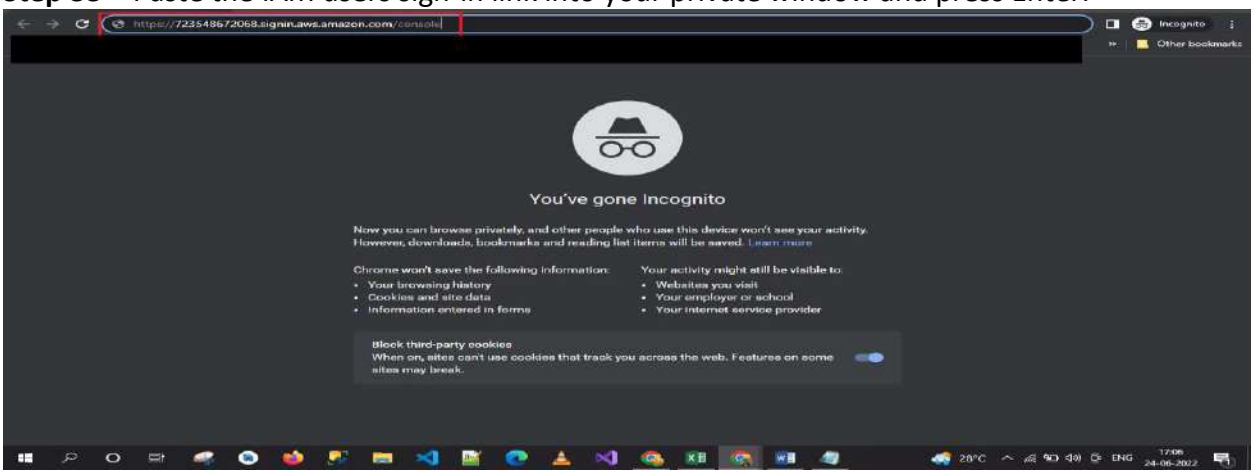
Microsoft Edge

- Click the ellipsis at the top-right of the screen
- Click New InPrivate window

Microsoft Internet Explorer

- Click the Tools menu option
- Click InPrivate Browsing

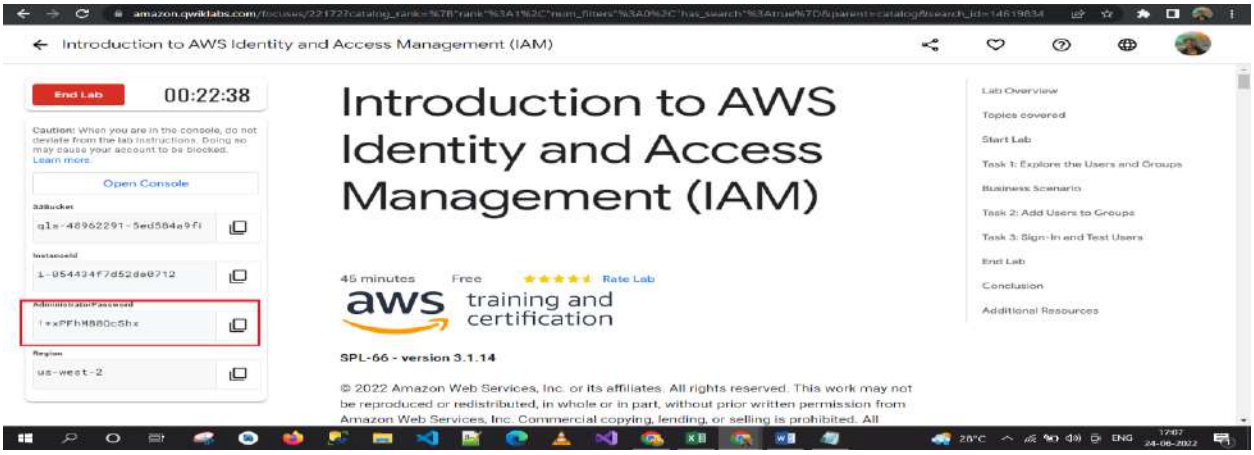
Step 33 – Paste the IAM users sign-in link into your private window and press Enter.

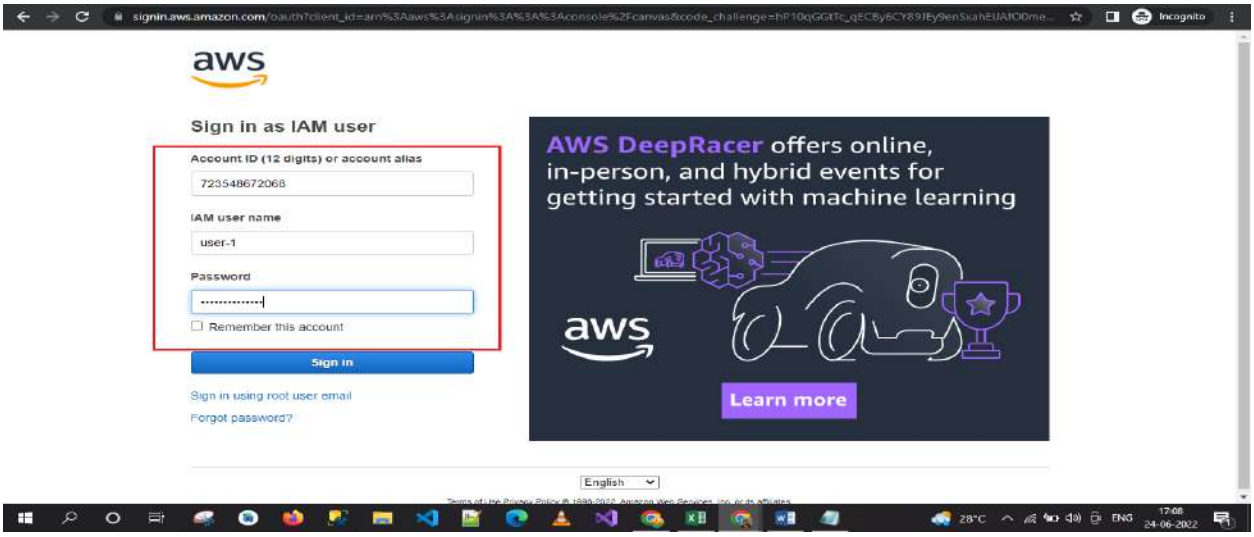


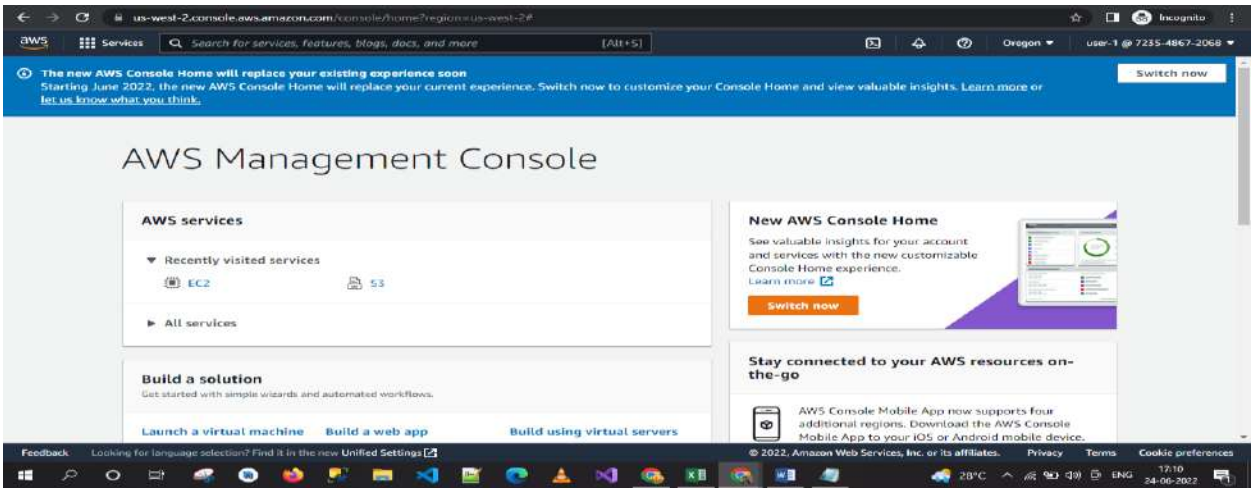
You will now sign-in as user-1, who has been hired as your Amazon S3 storage support staff.

Step 34 – Sign-in with: IAMusername: user-1

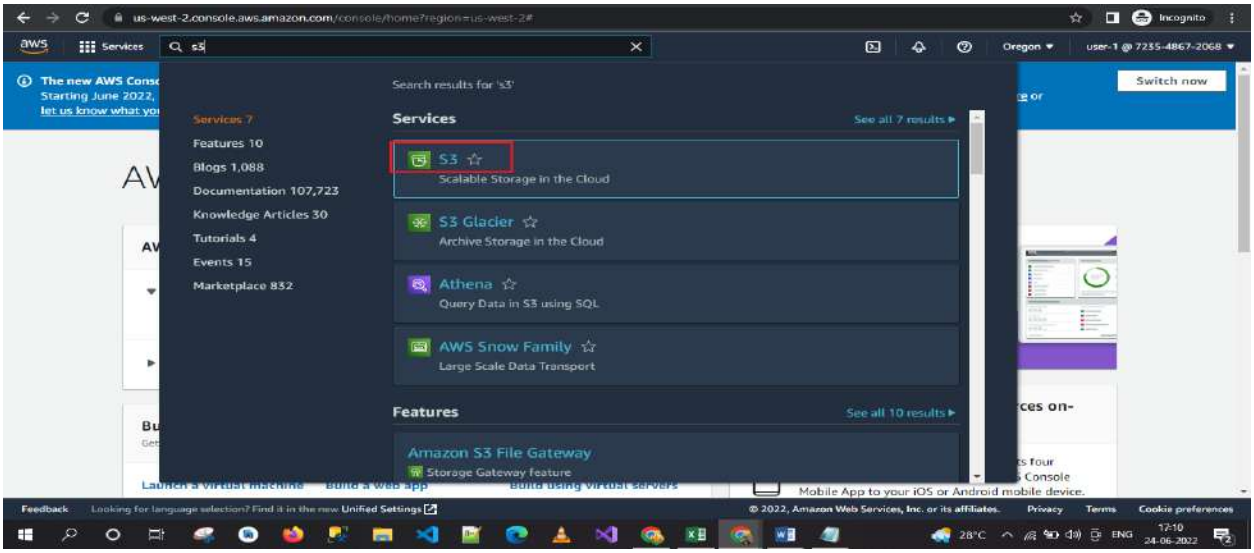
Password: Paste the value of AdministratorPassword located to the left of these instructions.



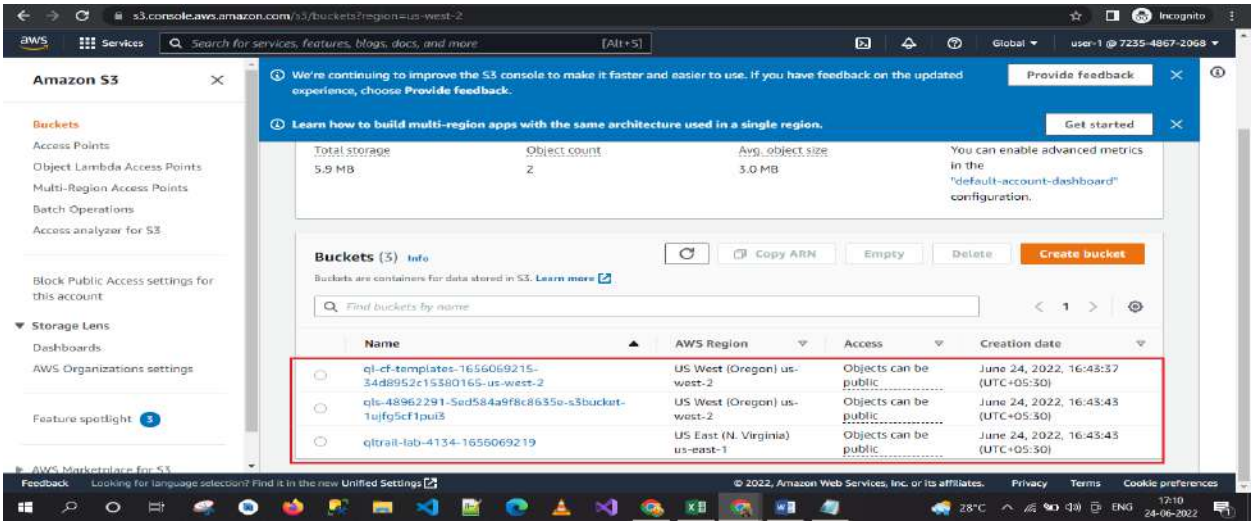


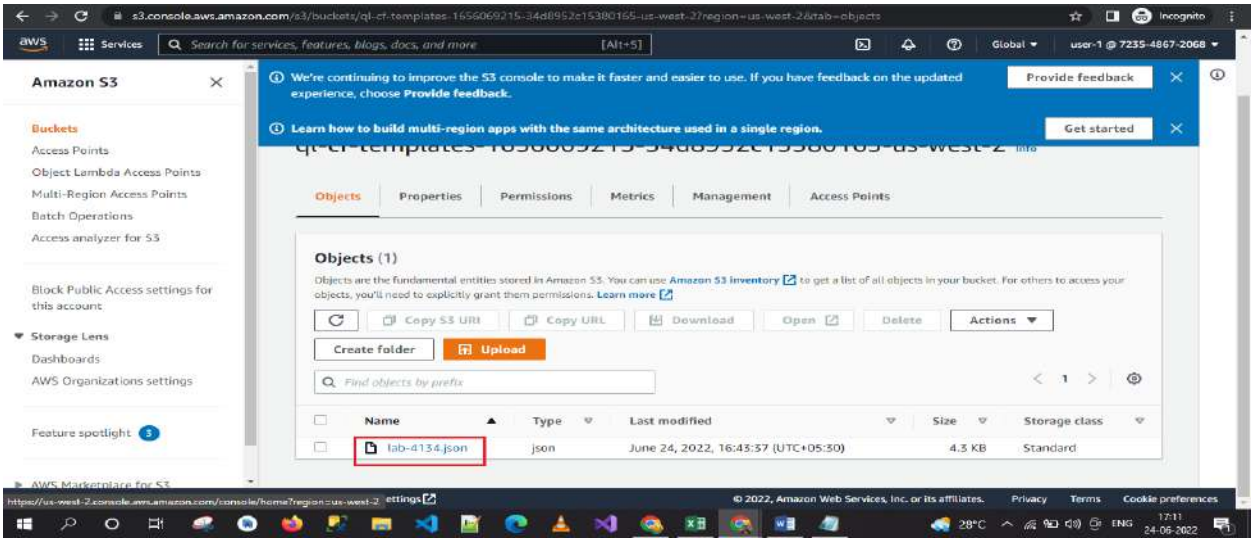


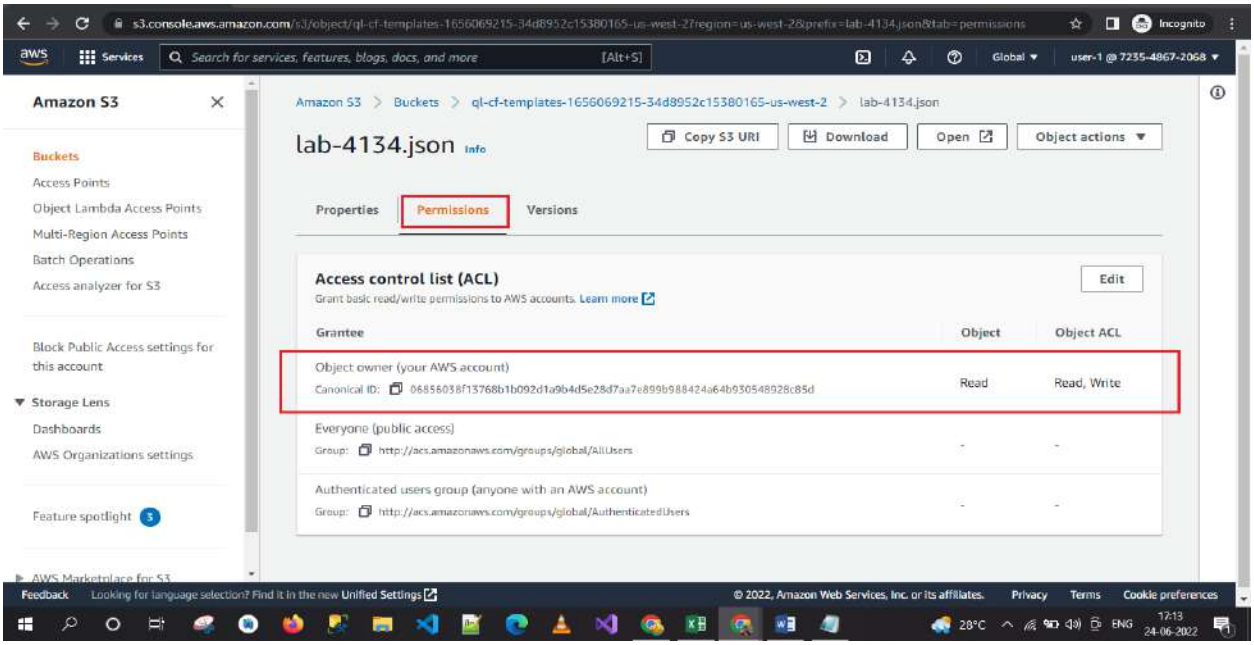
Step 35 – In the Services menu, click S3.



Step 36 – Click the name of one of your buckets and browse the contents.

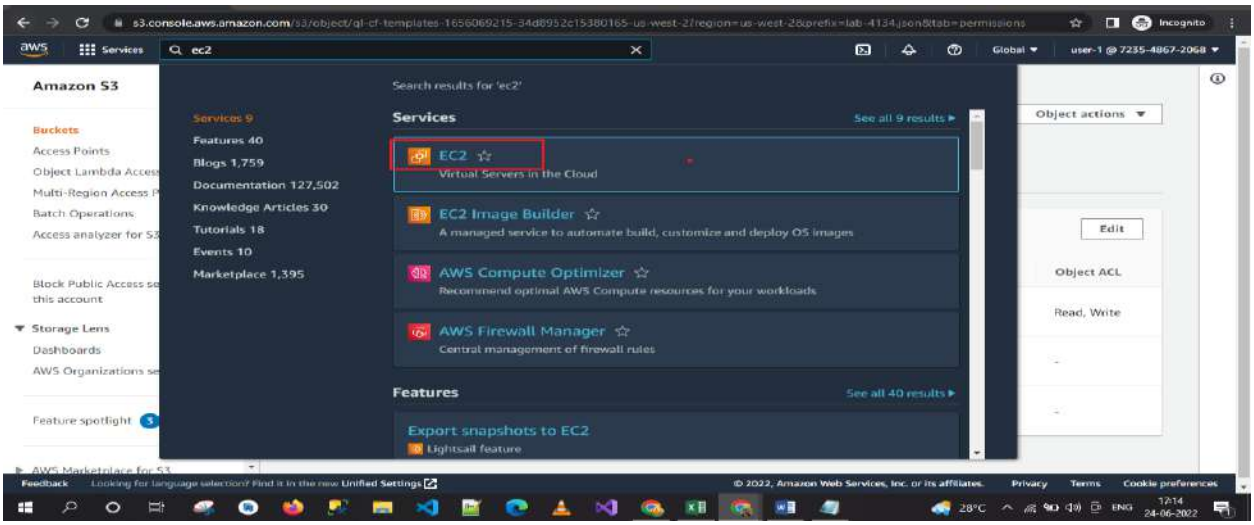






Since your user is part of the S3-Support Group in IAM, they have permission to view a list of Amazon S3 buckets and their contents. Now, test whether they have access to Amazon EC2.

Step 37 – In the Services menu, click EC2.

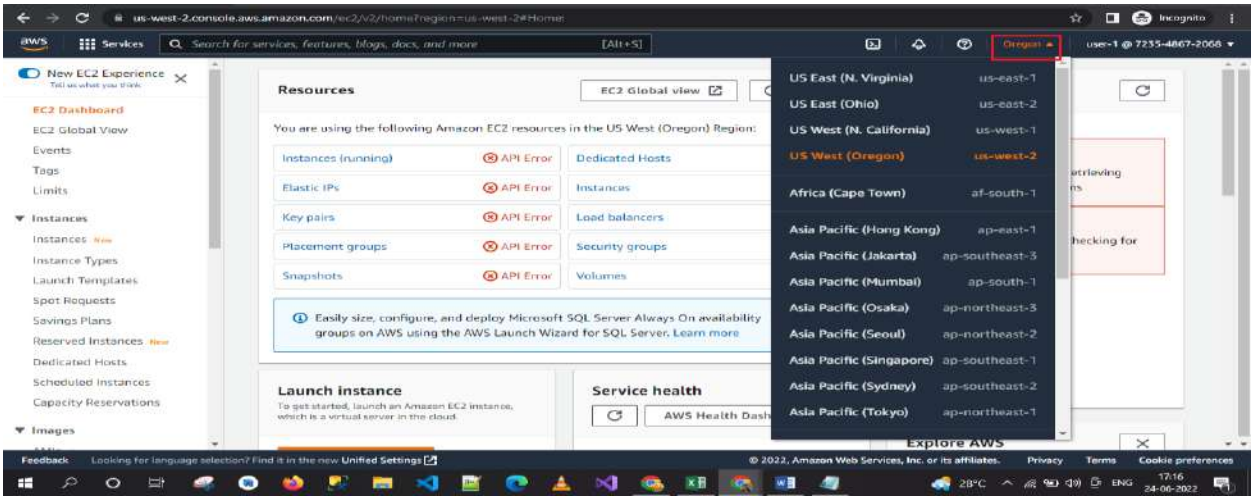


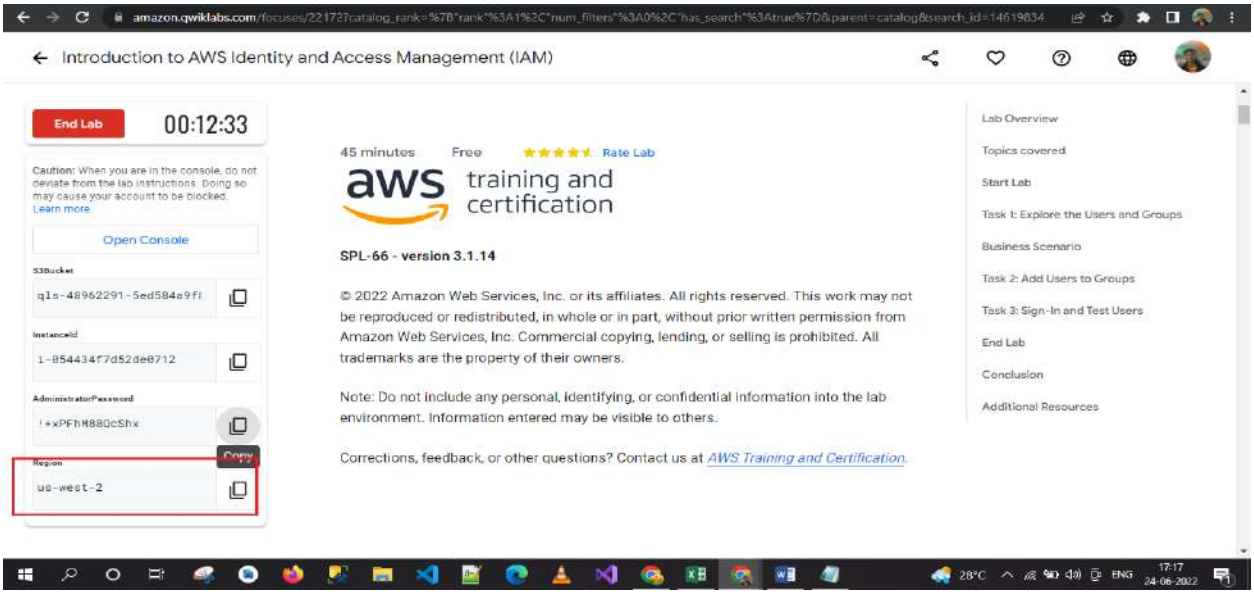
Login with new password and redo all the steps.

Step 38 – Navigate to the region that your lab was launched in by:

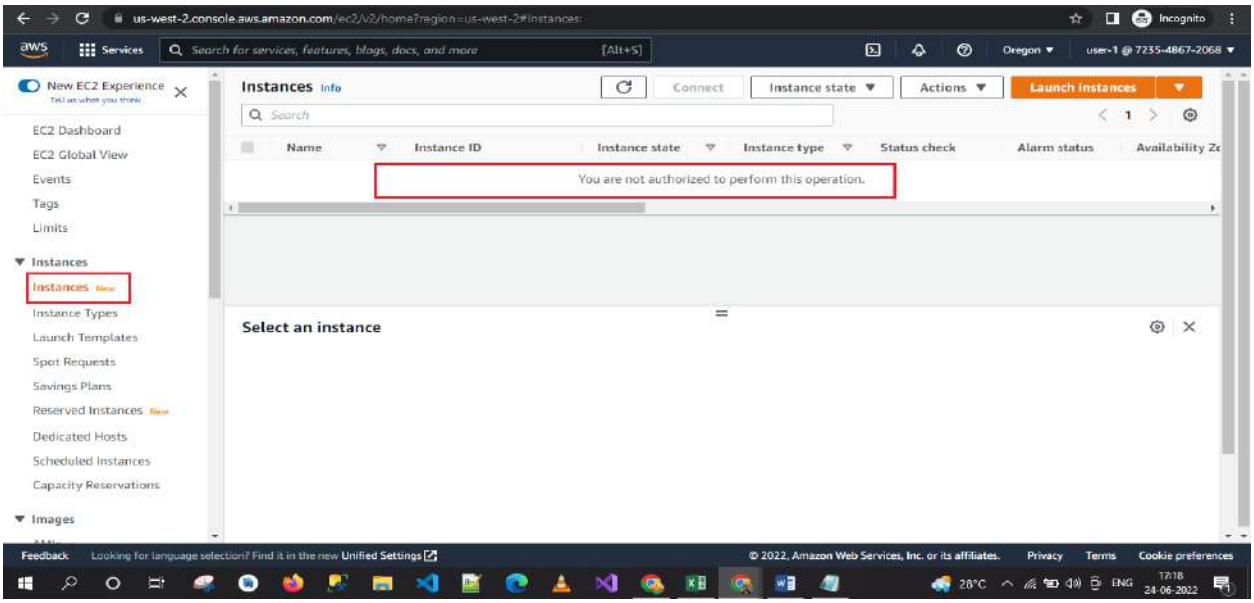
a. Clicking the drop-down arrow at the top of the screen, to the left of Support

b. Selecting the region value that matches the value of region to the left of these instructions



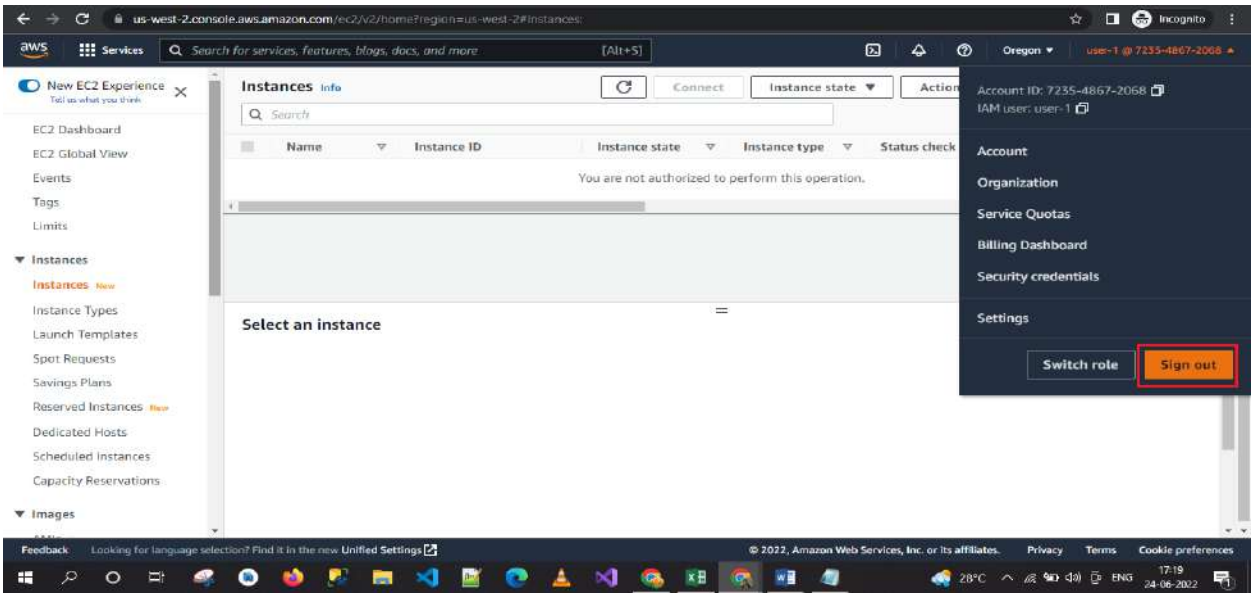


Step 39 – In the left navigation pane, click Instances.

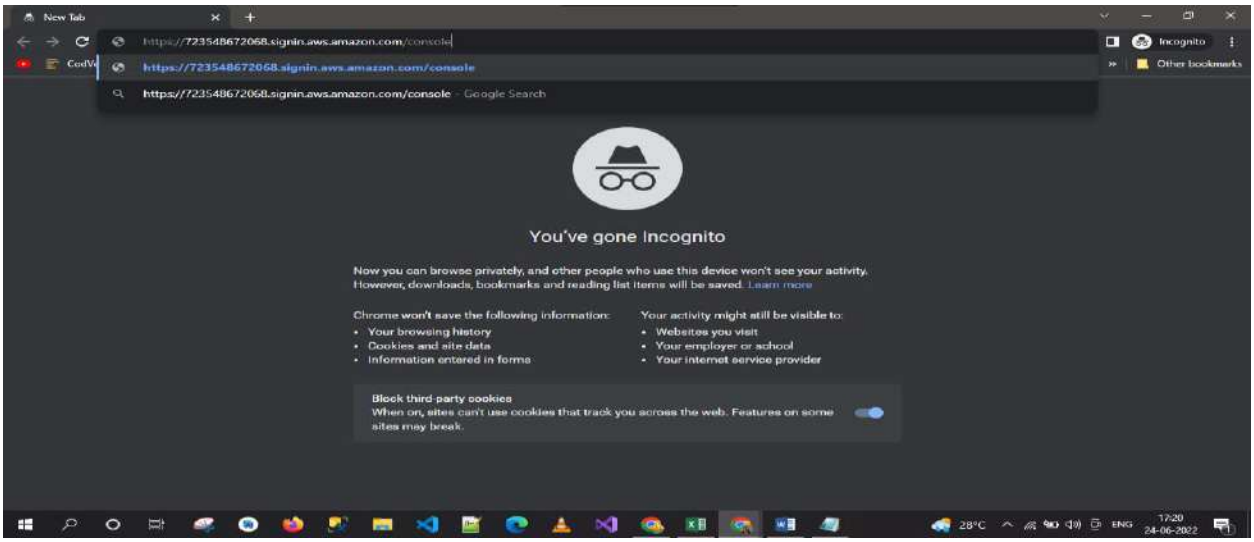


You cannot see any instances! Instead, it says an error occurred fetching instance data: You are not authorized to perform this operation... This is because your user has not been assigned any permissions to use Amazon EC2. You will now sign-in as user-2, who has been hired as your Amazon EC2 support person.

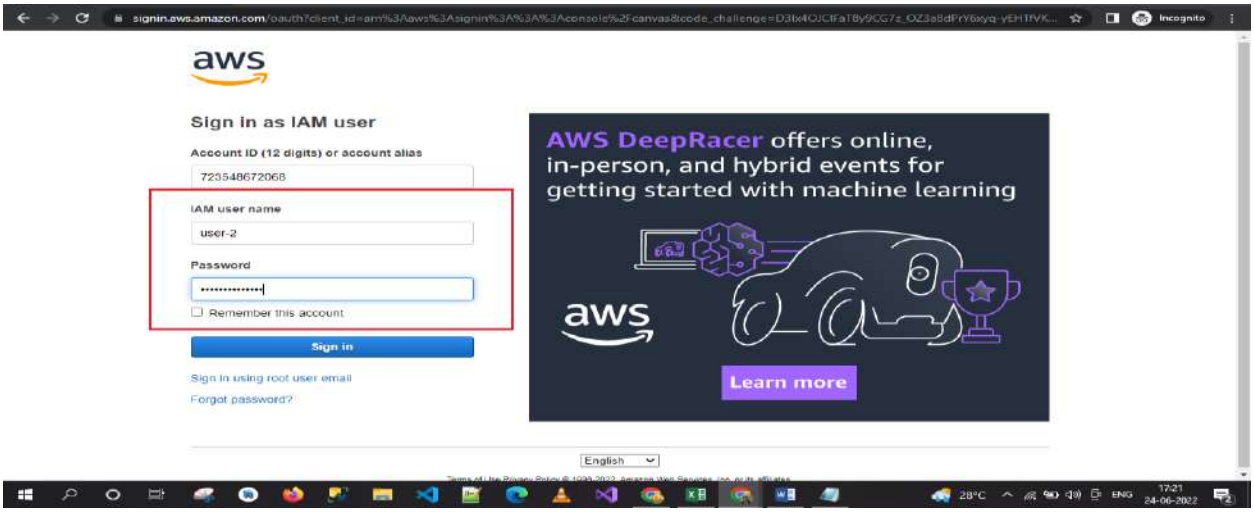
Step 40 – Sign user-1 out of the AWS Management Console by configuring the following:
a. At the top of the screen, click user-1
b. Click Sign Out



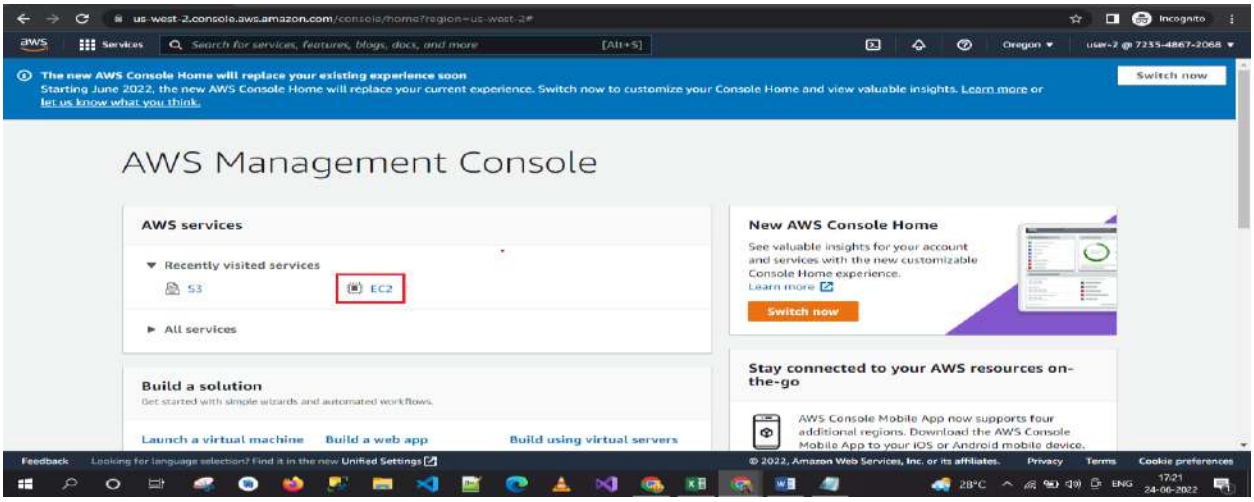
Step 41 – Paste the IAM users sign-in link into your private window and press Enter. This links should be in your text editor.



Step 42 – Sign-in with: IAMuser name: user-2 Password: Paste the value of AdministratorPassword located to the left of these instructions.



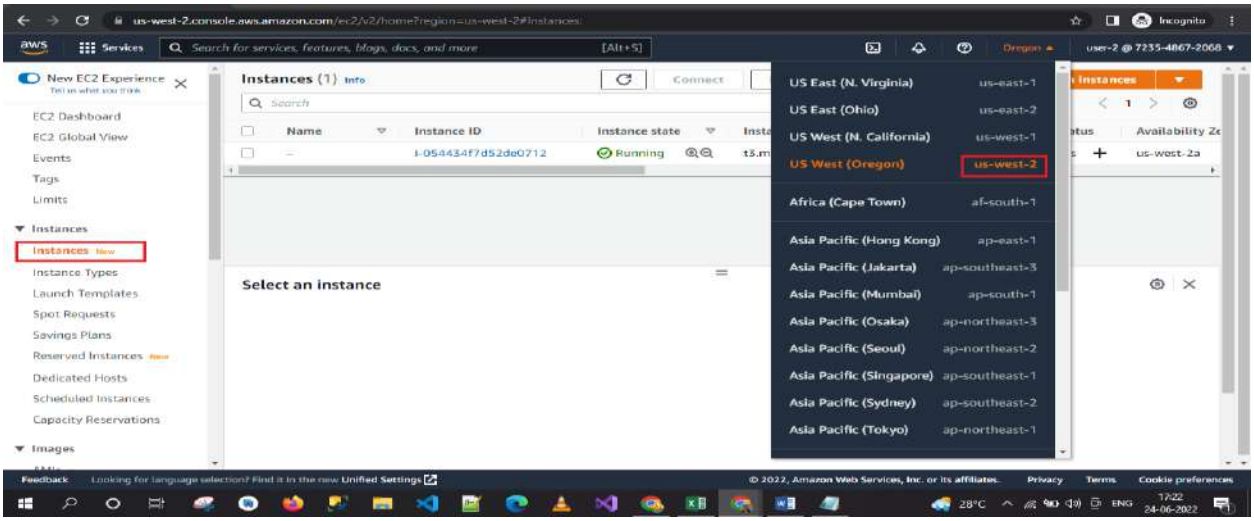
Step 43 – In the Services menu, click EC2.



Step 44 – Navigate to the region that your lab was launched in by:

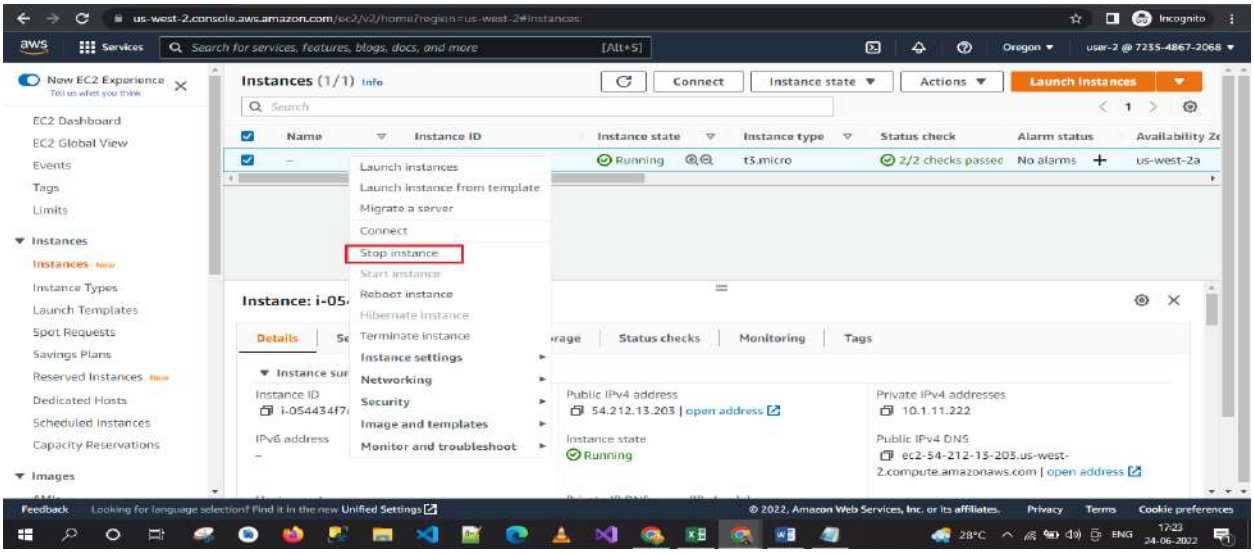
a. Clicking the drop-down arrow at the top of the screen, to the left of Support

b. Selecting the region value that matches the value of Region to the left of these instructions

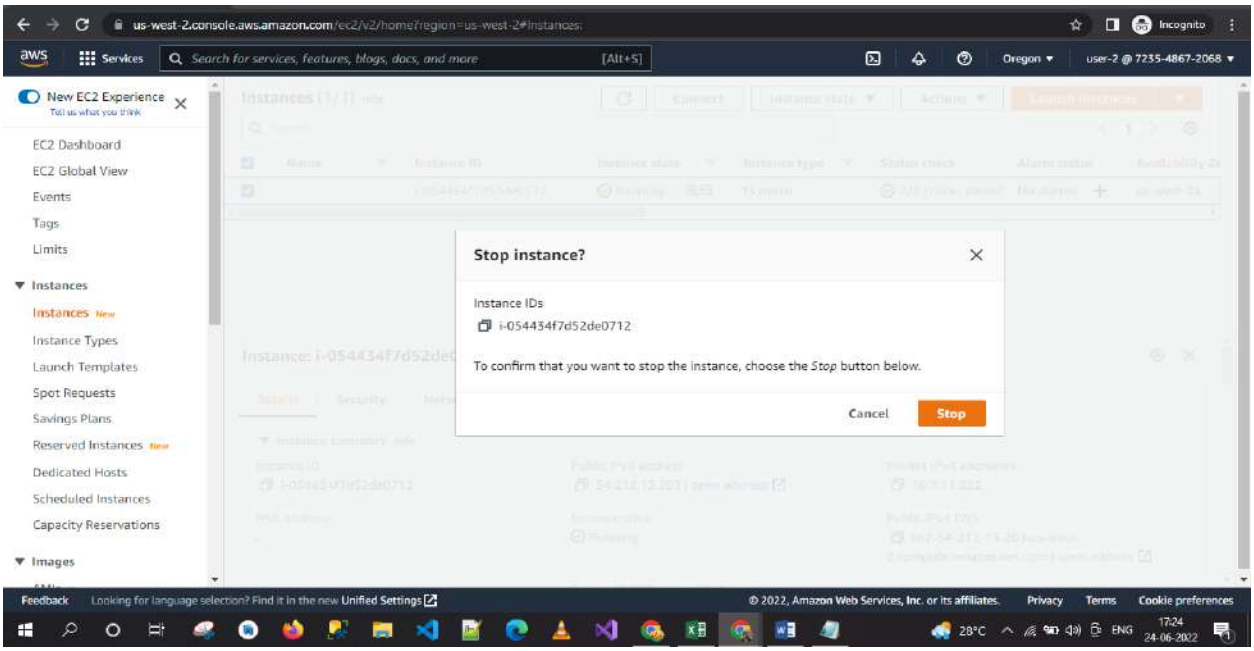


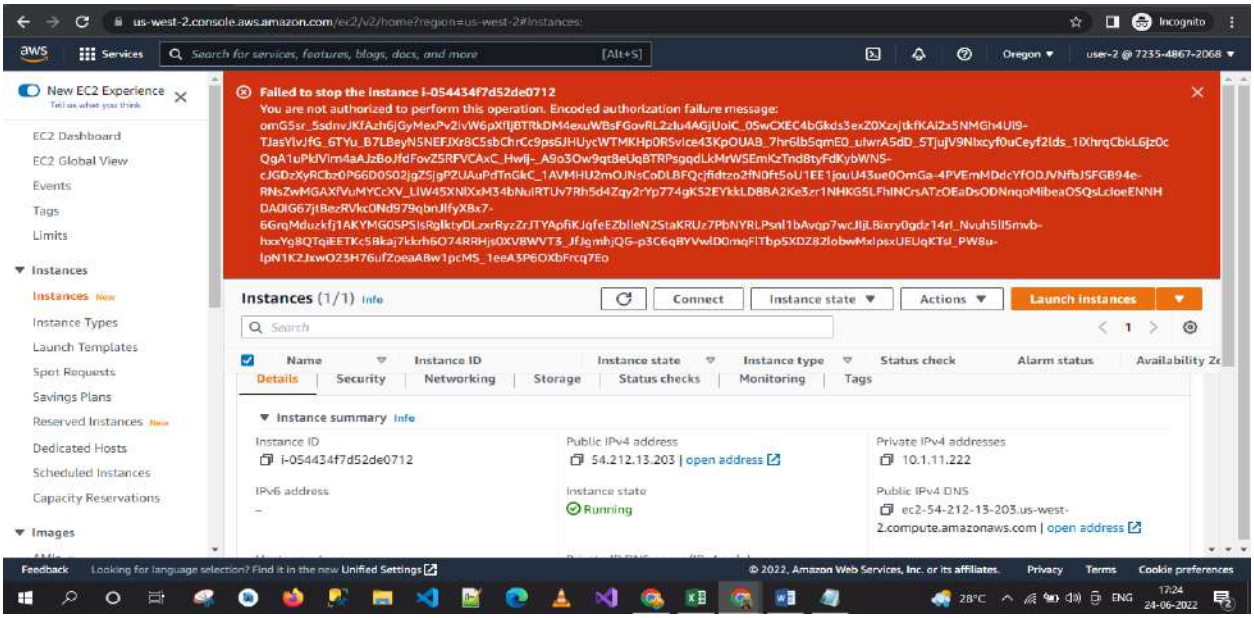
Step 45 – You are now able to see an Amazon EC2 instance because you have Read Only permissions. However, you will not be able to make any changes to Amazon EC2 resources.

Your EC2 instance should be selected. If it is not selected, select it.



Step 46 – In the Actions menu, click Instance State > Stop.

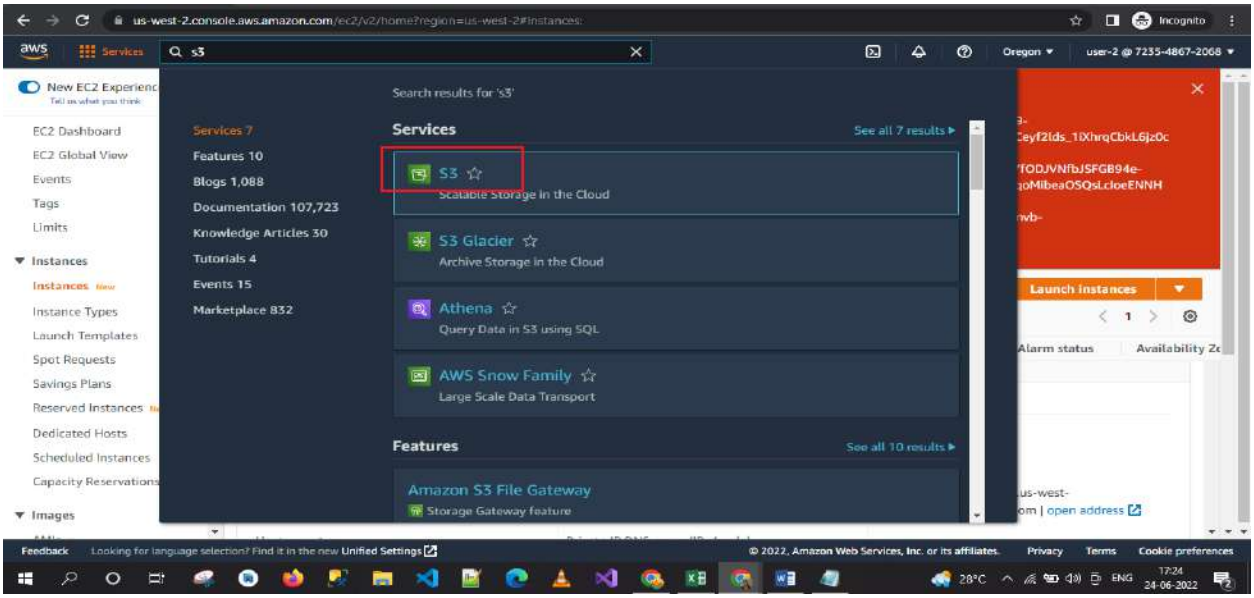


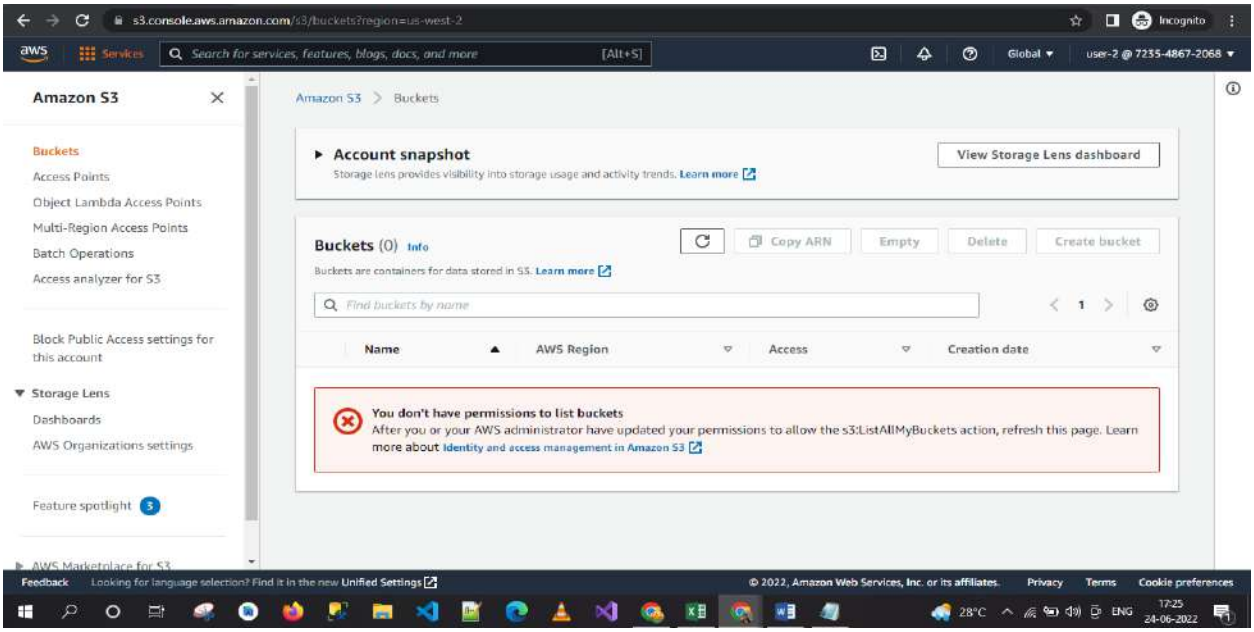


You will receive an error stating You are not authorized to perform this operation. This demonstrates that the policy only allows you to information, without making changes.

Step 47 – At the Stop Instances window, click Cancel. Next, check if user-2 can access Amazon S3.

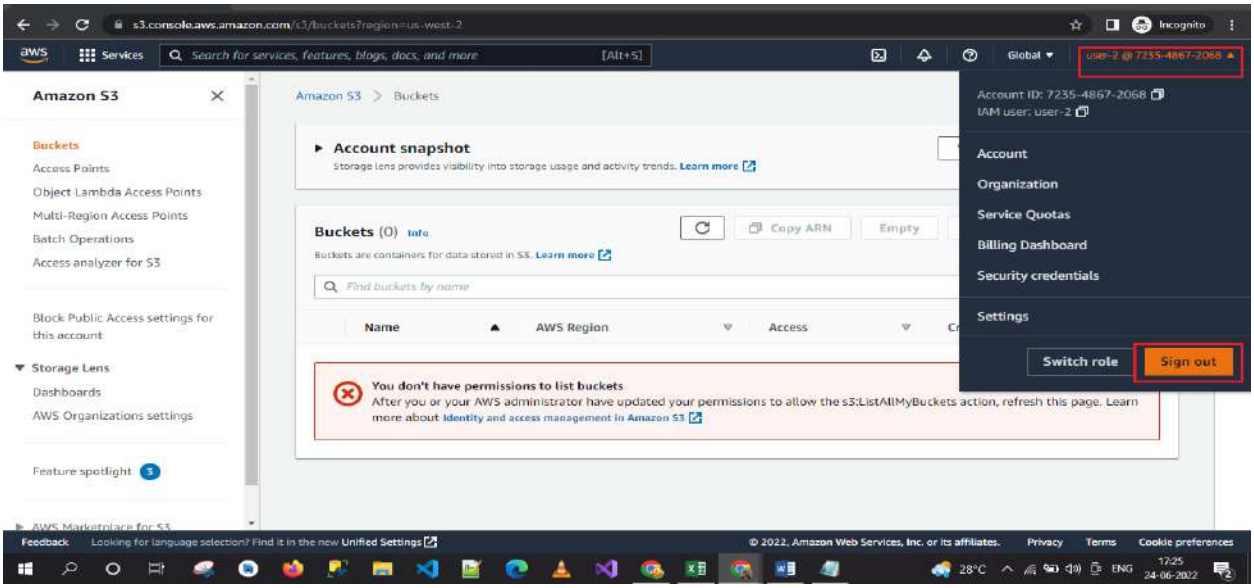
Step 48 – In the Services, click S3. You will receive an Error has Denied because user-2 does not have permission to use Amazon S3





You will now sign-in as user-3, who has been hired as your Amazon EC2 administrator.

Step 49 – Sign user-2 out of the AWS Management Console by configuring the following:
a. At the top of the screen, click user-2.
b. Click Sign Out.

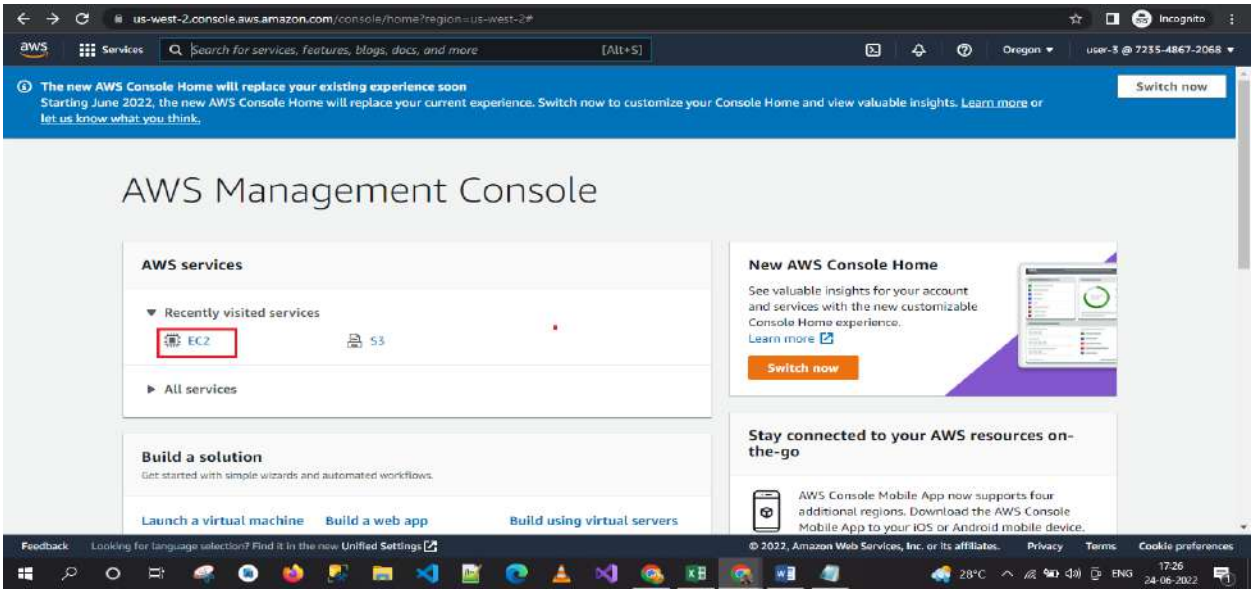


Step 50 – Paste the IAM users sign-in link into your private window and press Enter.

Step 51 – Paste the sign-in link into your web browser address bar again. If it is not in your clipboard, retrieve it from the text editor where you stored it earlier.

Step 52 – Sign-in with: IAM username: user-3 Password: Paste the value of AdministratorPassword located to the left of these instructions.

Step 53 – In the Services menu, click EC2.



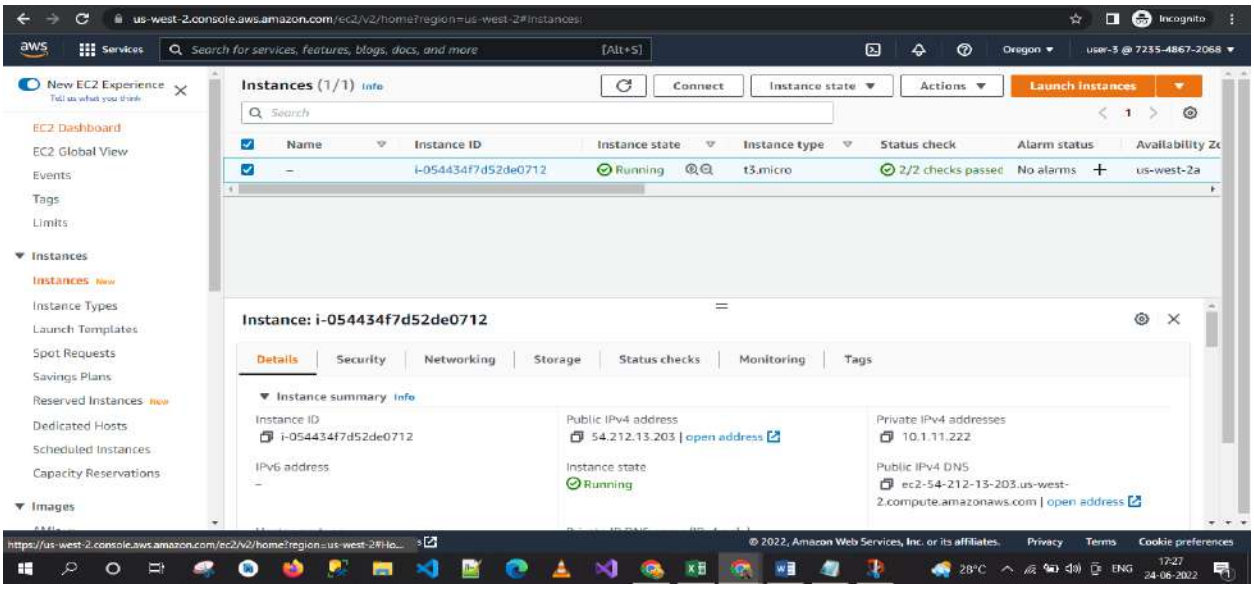
Step 54 – Navigate to the region that your lab was launched in by:

a. Clicking the drop-down arrow at the top of the screen, to the left of Support

b. Selecting the region value that matches the value of Region to the left of these instructions

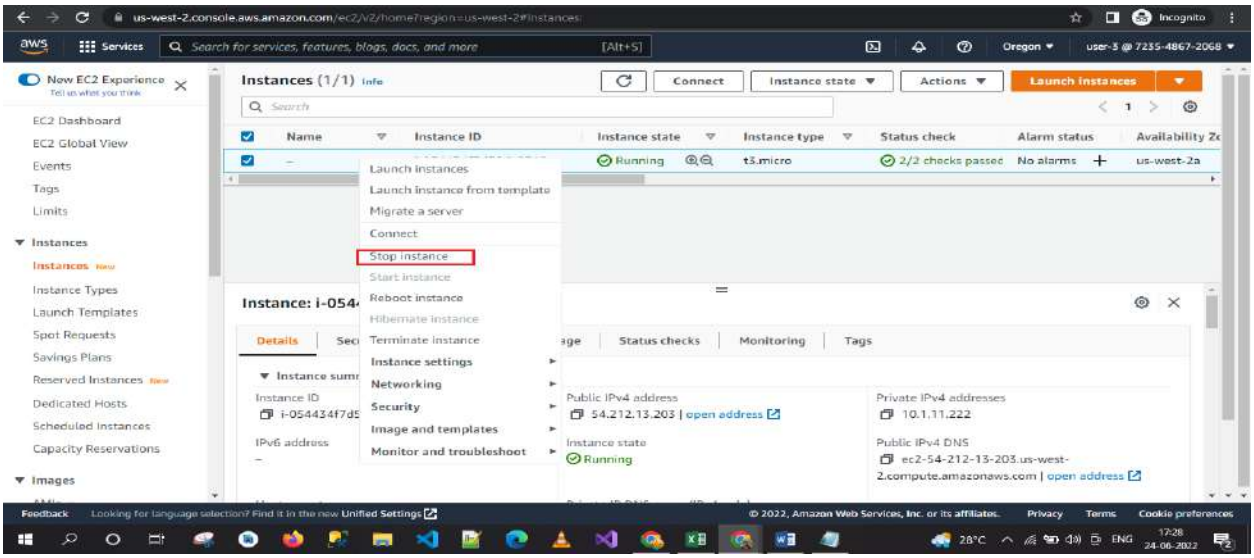
Step 55 – In the navigation pane on the left, click Instances.

As an EC2 Administrator, you should now have permissions to Stop the Amazon EC2 instance. Your EC2 instance should be selected. If it is not, please select it

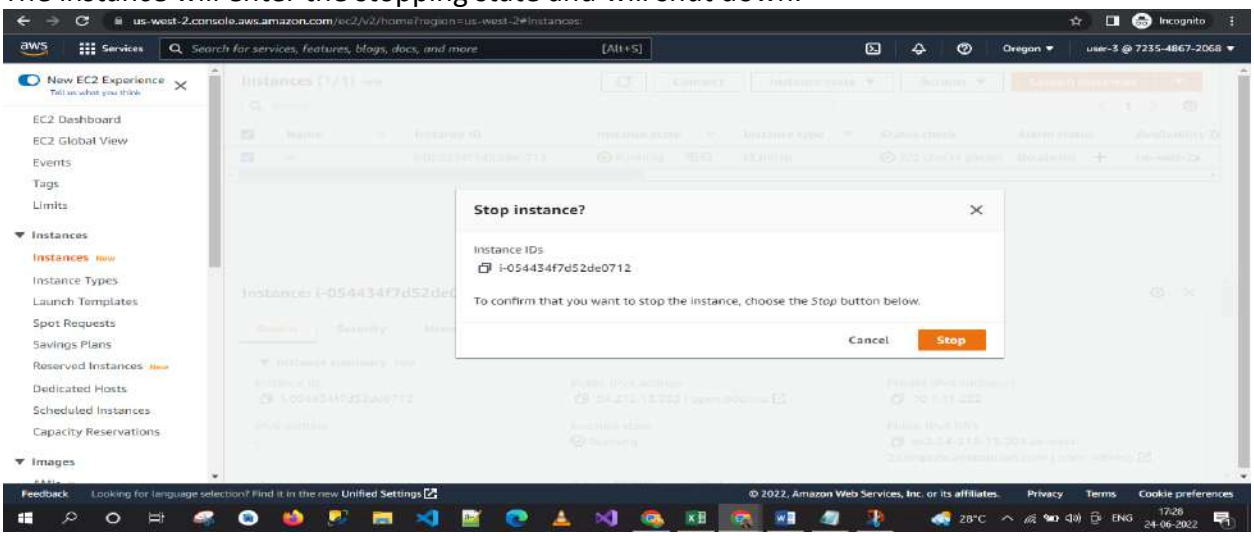


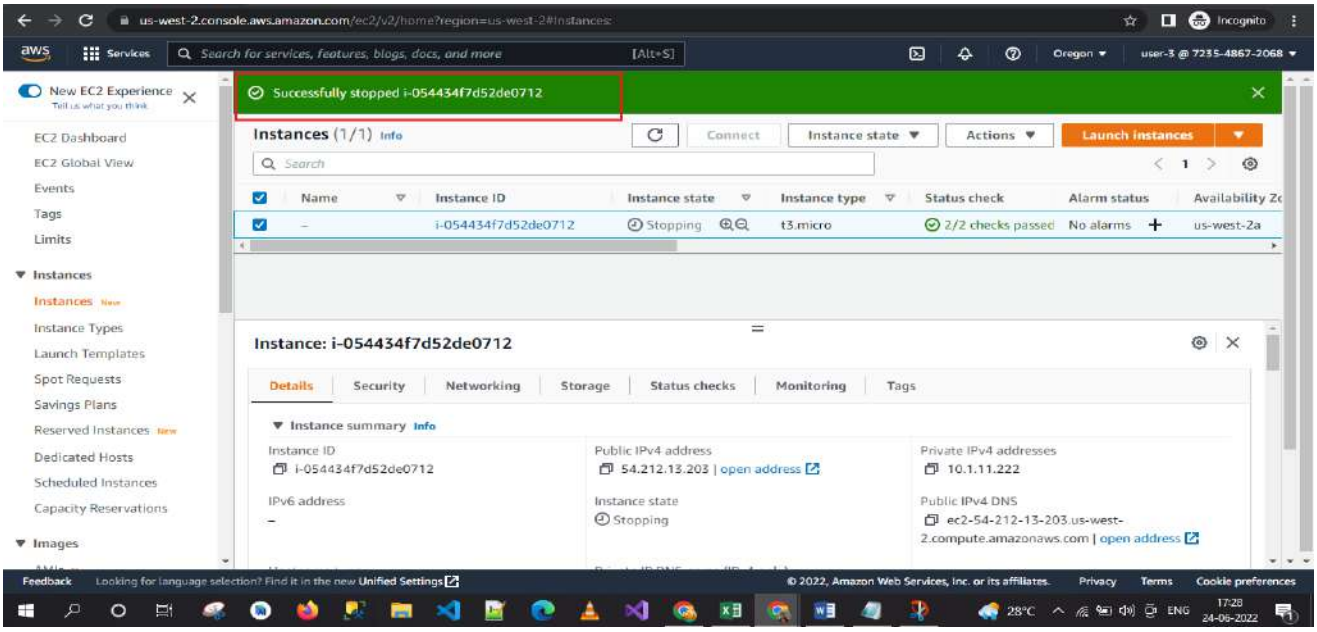
Step 56 – In the Actions menu, click Instance State > Stop

Right Click on the Instance and Click on the Stop instance

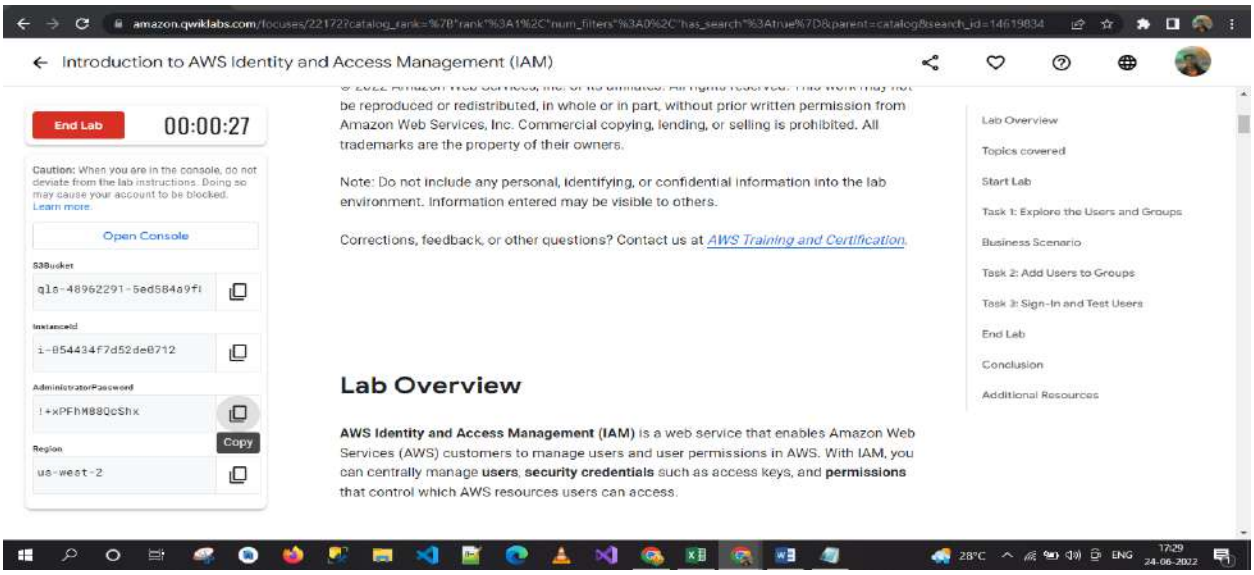


Step 57 – In the Stop Instances window, click Yes, Stop.
The instance will enter the stopping state and will shut down.





Step 58 – Close your private window. End Lab Follow these steps to close the console, end your lab, and evaluate the experience.



Step 59 –Return to the AWS Management Console.

Step 60 –On the navigation bar, click awsstudent@, and then click Sign Out. 62. click End Lab

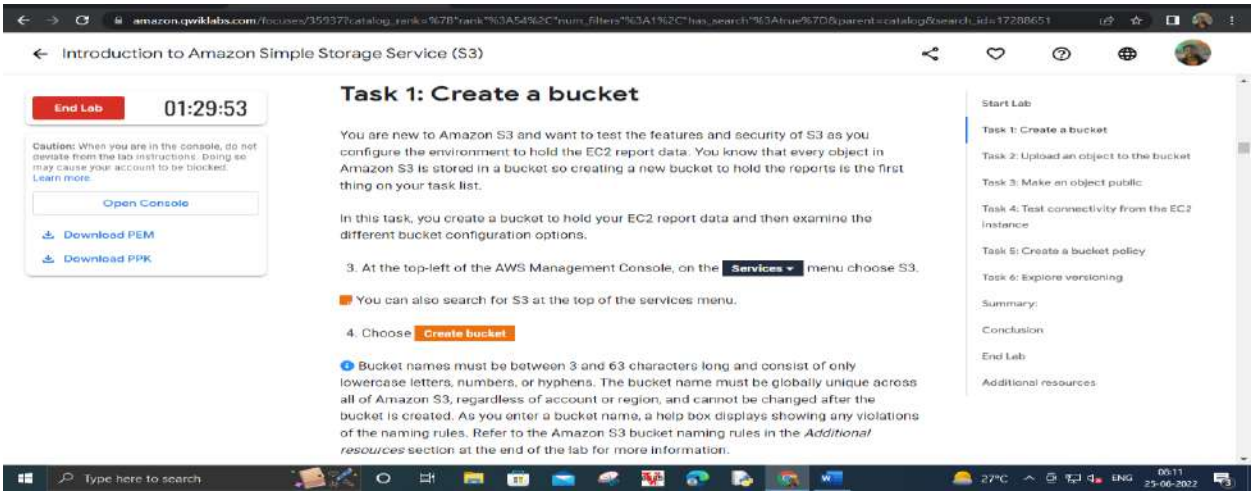
Practical 3: Working with S3 Buckets

A. Create a Bucket
B. Upload an object to the bucket
C. Make an Object public
D. Create a bucket policy
E. Explore versioning

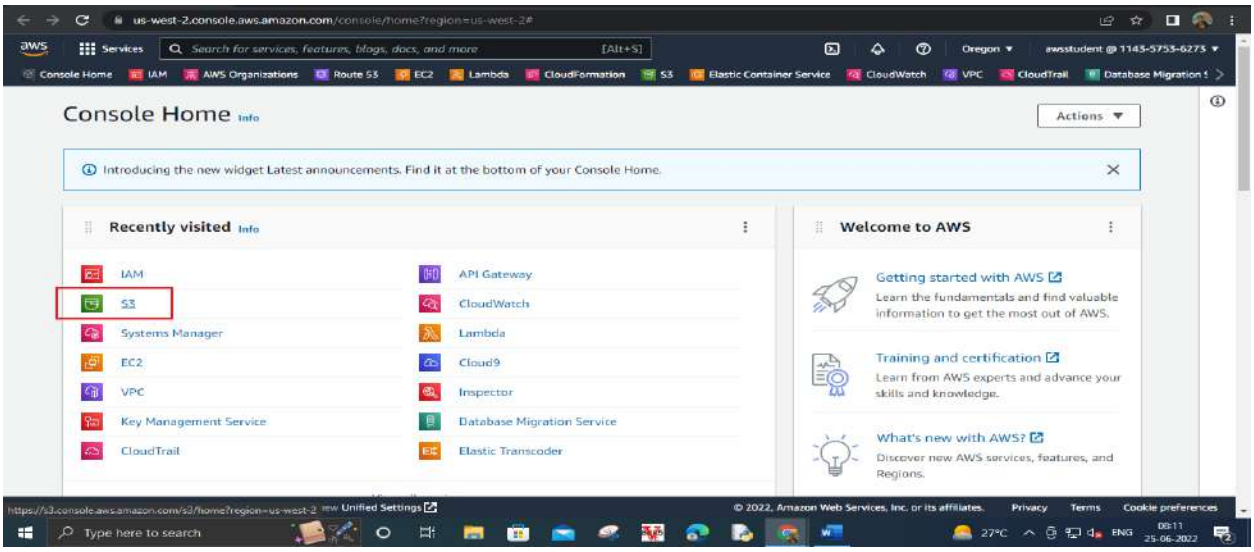
Task 1: Create a bucket

Step 1 –Click Start Lab

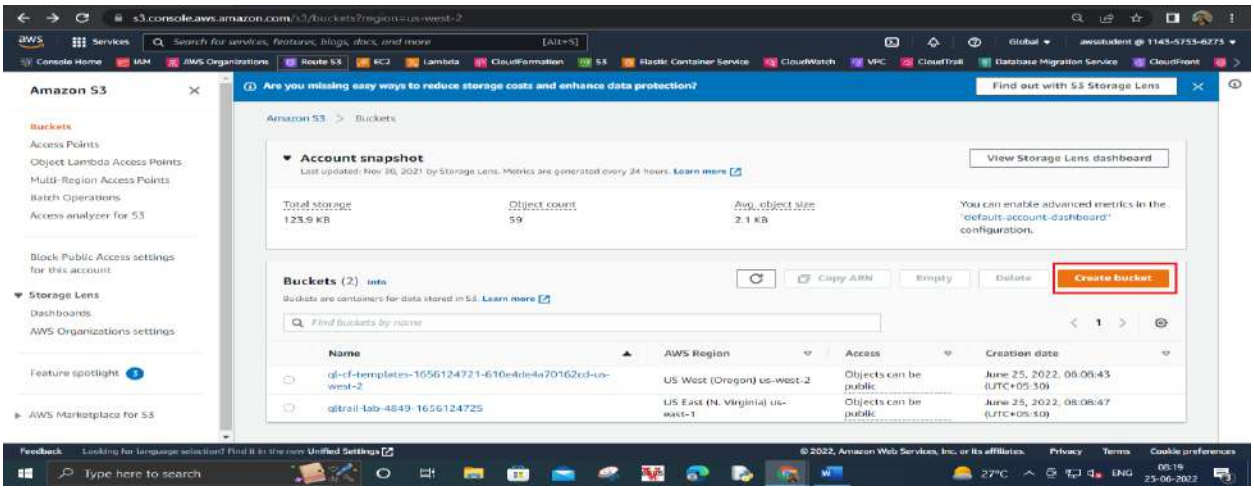
Step 2 – Click on Open Console



Step 2 – Click on S3 services OR Go to the Services and select the S3 Service OR Search by the Search box



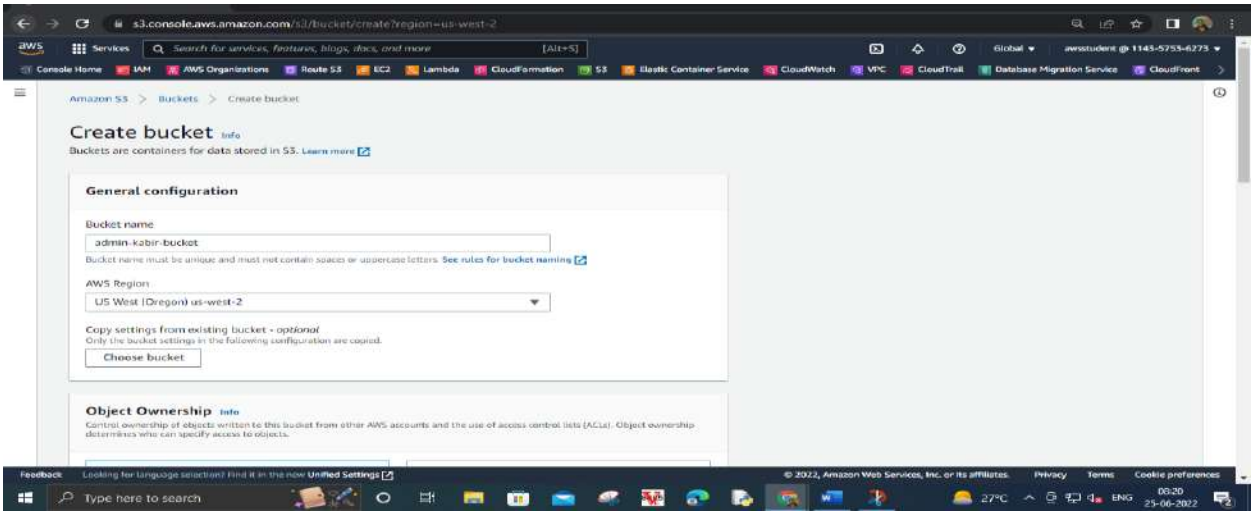
Step 3 – Choose create bucket.



Step 4 – Under the General configuration section, name your bucket.

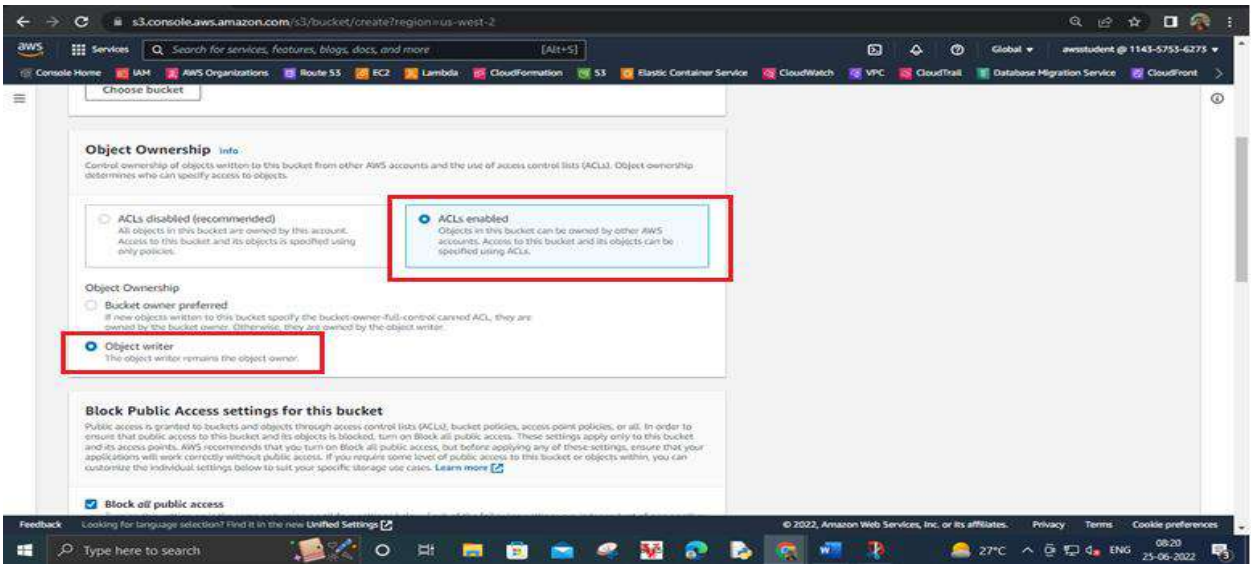
Replace in the bucket name with a random number. This ensures that you have a unique name.

* Example Bucket Name - admin-kabir-bucket987987



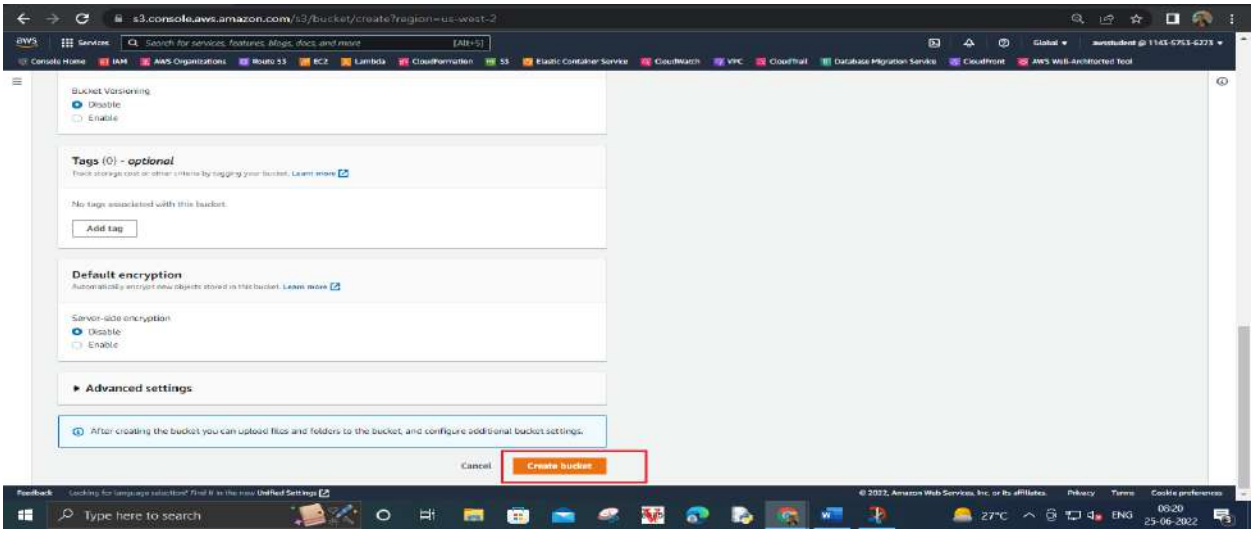
Step 5 – In the **Object Ownership** section, configure:

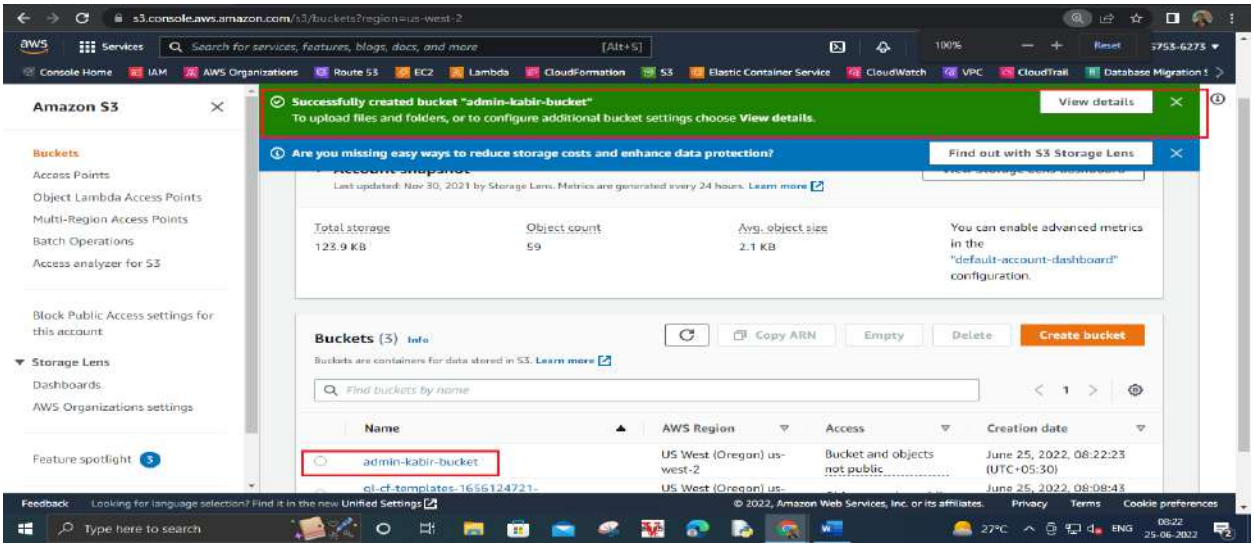
- ACLs enabled
- Object Writer



Step 6 – Leave Region as it defaults value.

Step 7 – Scroll to the bottom and choose **Create Bucket.**



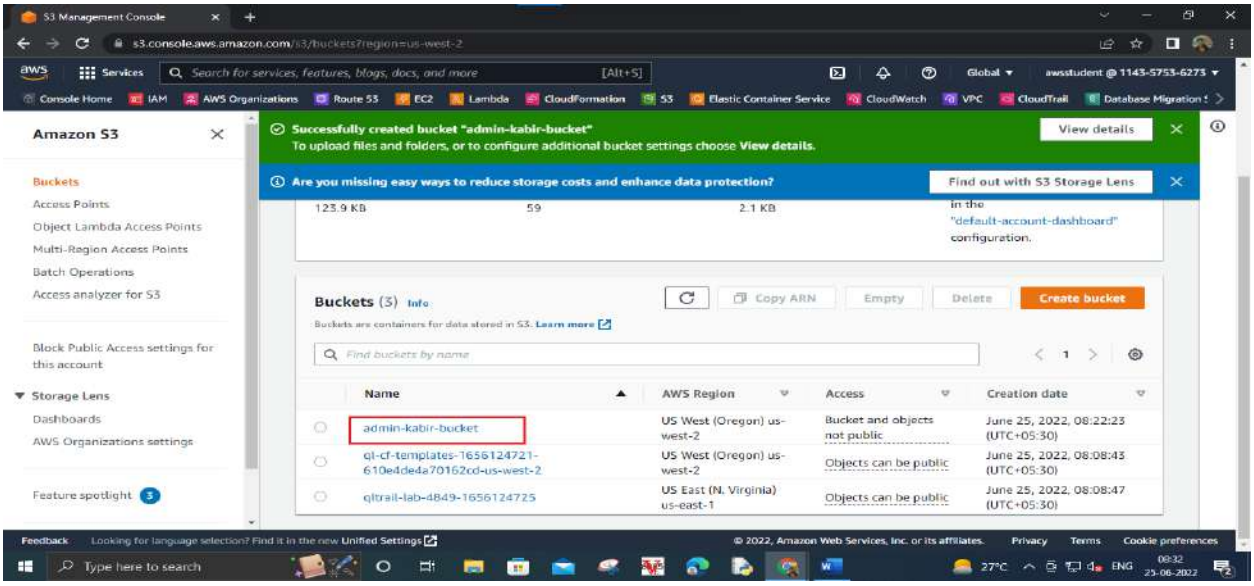


Task 2: Upload an object to the bucket

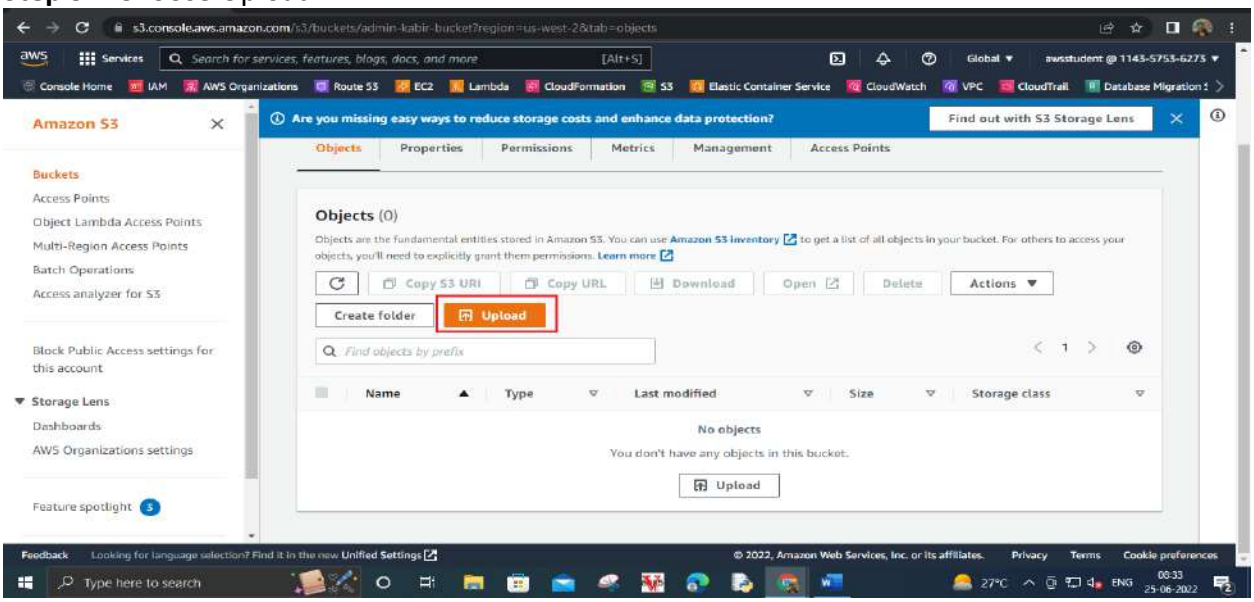
Now that you have a bucket created for your report data, you are ready to work with objects. An object can be any kind of file: a text file, a photo, a video, a zip file, and so on. When you add an object to Amazon S3, you have the option of including metadata with the object and setting permissions to control access to the object.

In this task you test uploading objects to your admin-kabir-bucket. You have a screen capture of a daily report and want to upload this image to your S3 bucket.

Step 8 – Click the In the S3 Management Console, find and select the bucket that starts with the name admin-kabir-bucket.

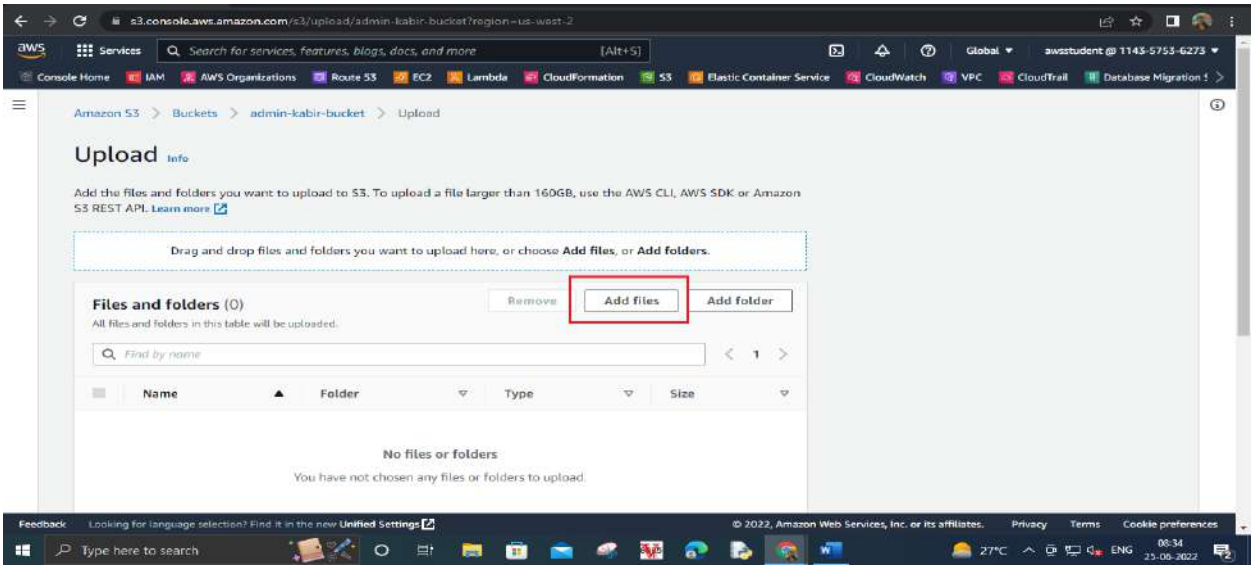


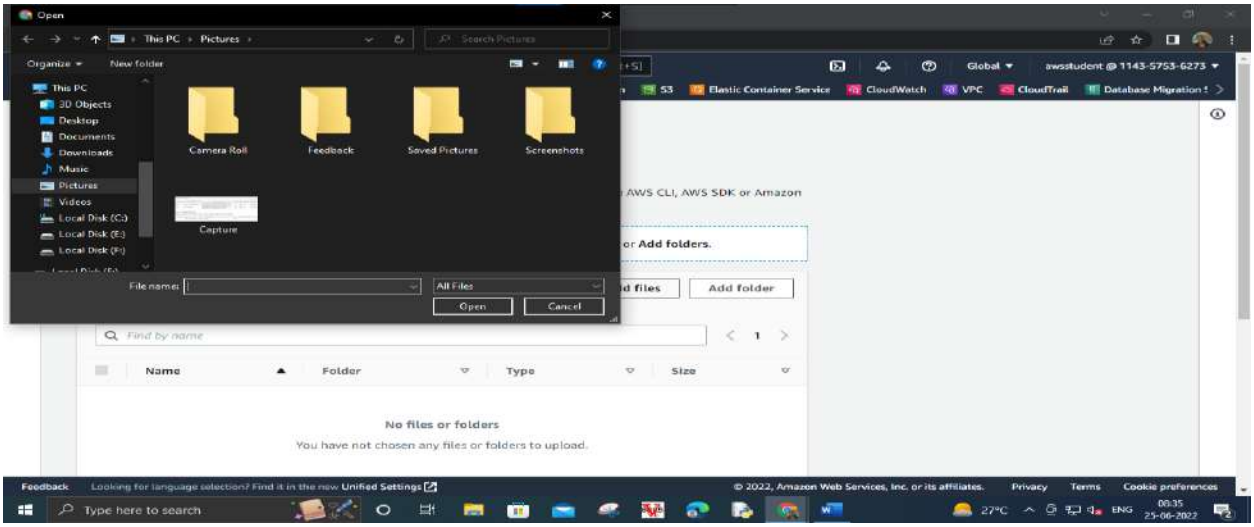
Step 9 – Choose Upload.



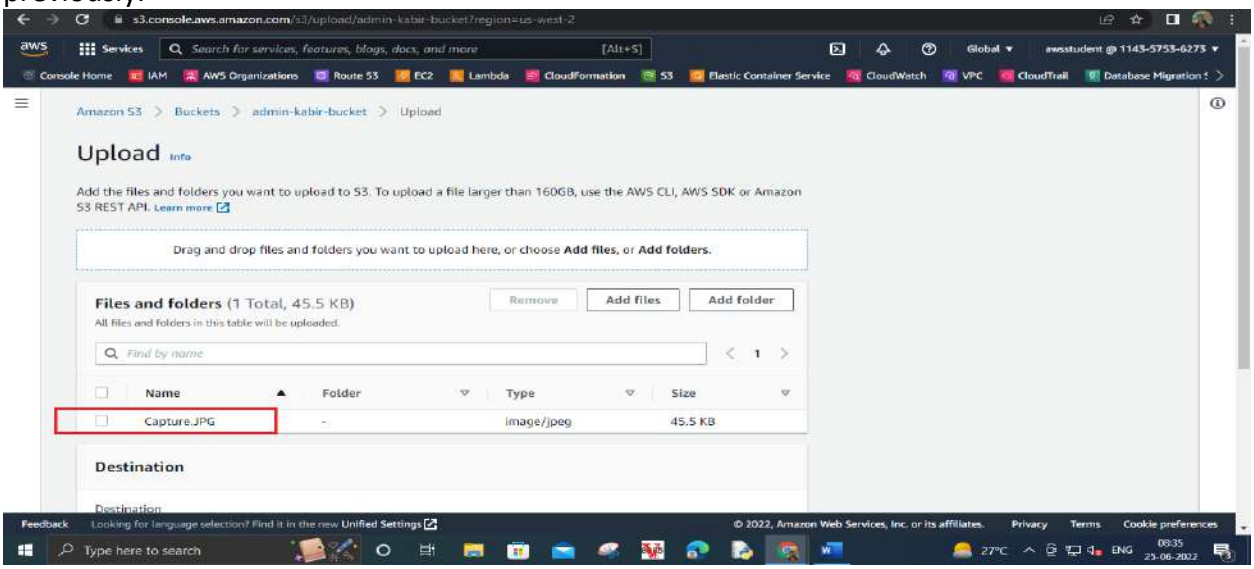
This launches an upload wizard. Use this wizard to upload files either by selecting them from a file chooser or by dragging them to the S3 window.

Step 10 – Choose Add files.

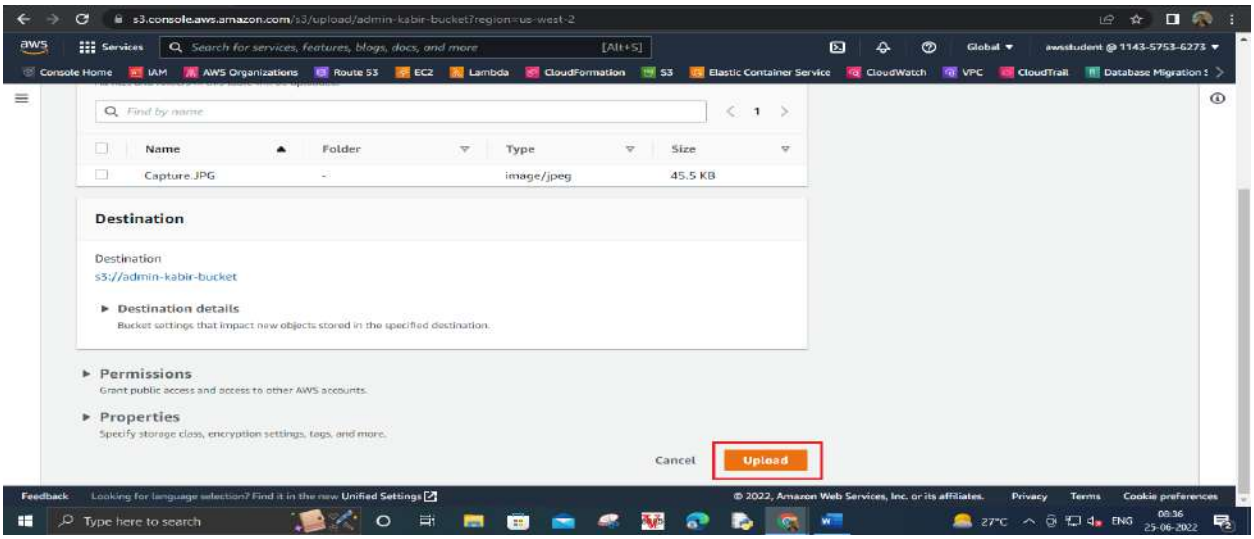


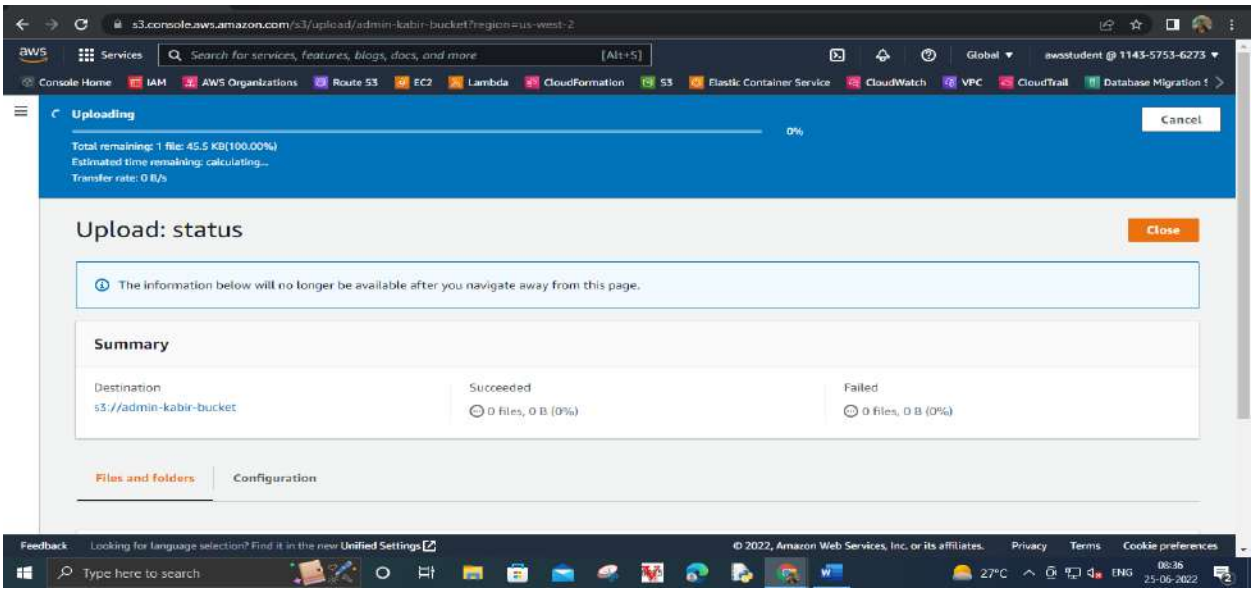


Step 11 – Click the EC2-Support group Browse to and select the file that you downloaded previously.

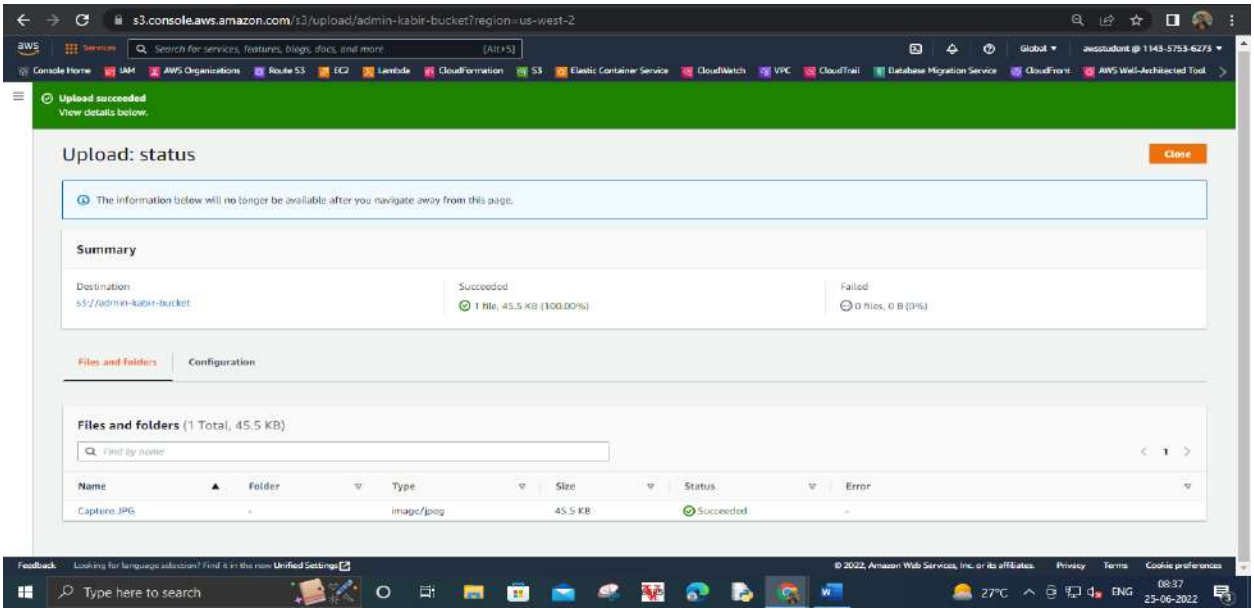


Step 11 – Scroll down and choose **Upload**.





Your file is successfully uploaded when the green bar indicating Upload succeeded appears.



In the Upload: status section, choose close.

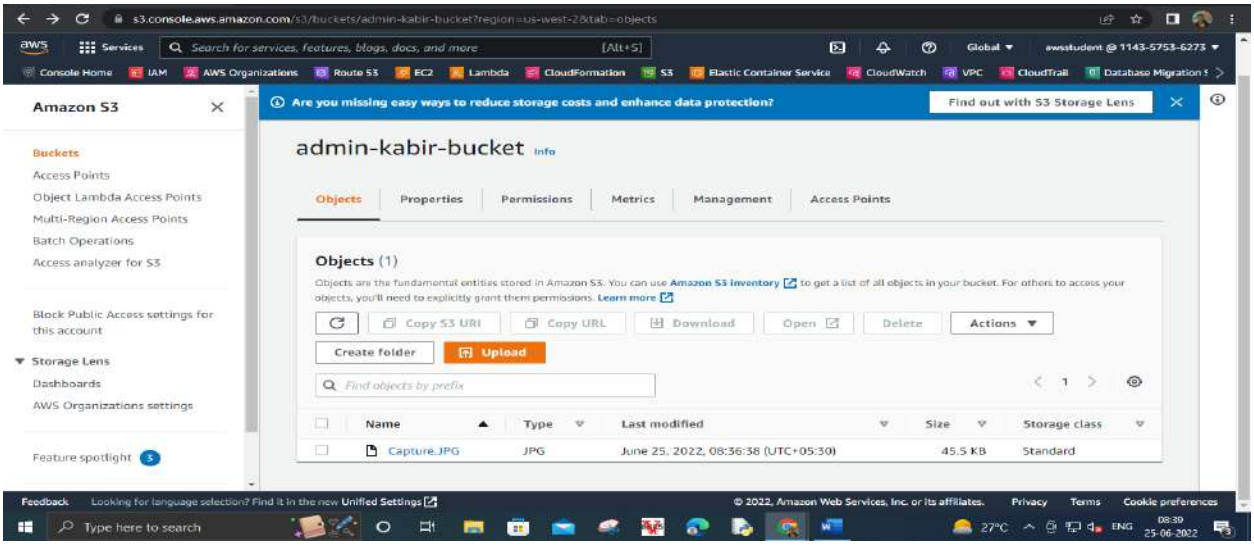
Task 3: Make an Object public

Security is a priority in Amazon S3. Before you configure your EC2 instance to connect to the admin-kabir-bucket, you want to test the bucket and object settings for security.

In this task, you configure permissions on your bucket and your object to test accessibility.

First, you attempt to access the object to confirm that it is private by default.

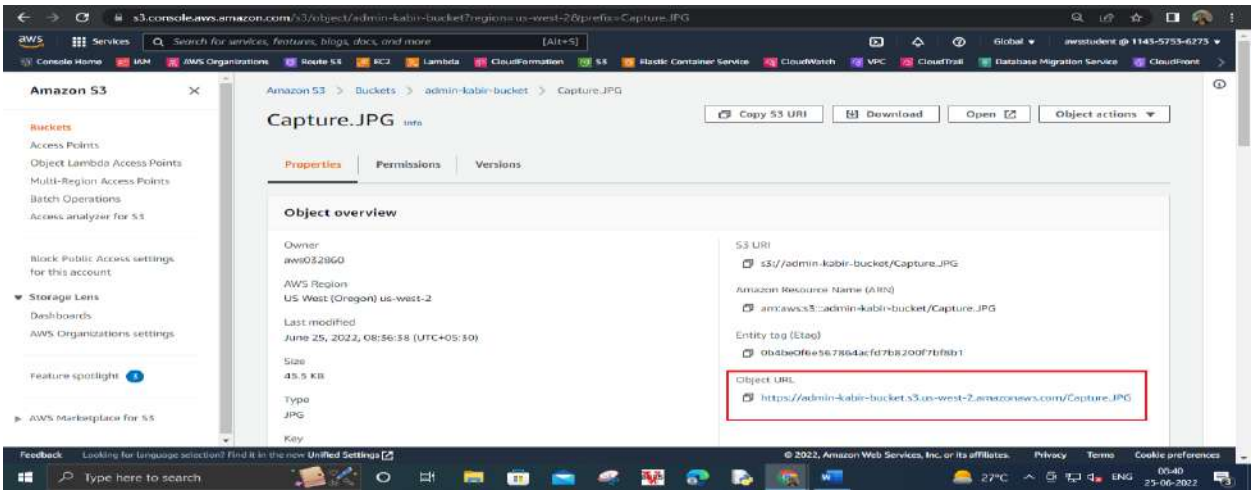
Step 12 – In the bucket overview page, on the objects tab, locate the object, and choose the file name.



The Capture.png overview page opens. Notice that the navigation in the top-left updates with a link to return to the bucket overview page.

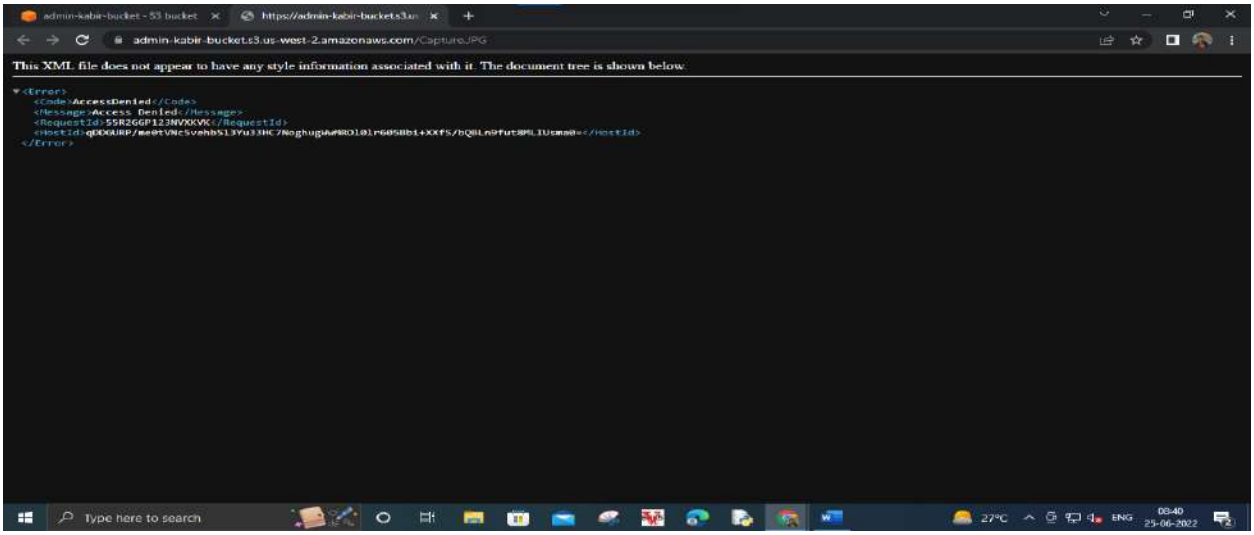
Step 13 – In the Object overview section, locate and copy the Object URL link.

https://admin-kabir-bucket.s3.us-west-2.amazonaws.com/Capture.JPG



Step 14 – Open a new browser tab and paste the Object URL link into the address field, and then press Enter.

You receive an Access Denied error. This is because objects in Amazon S3 are private by default.



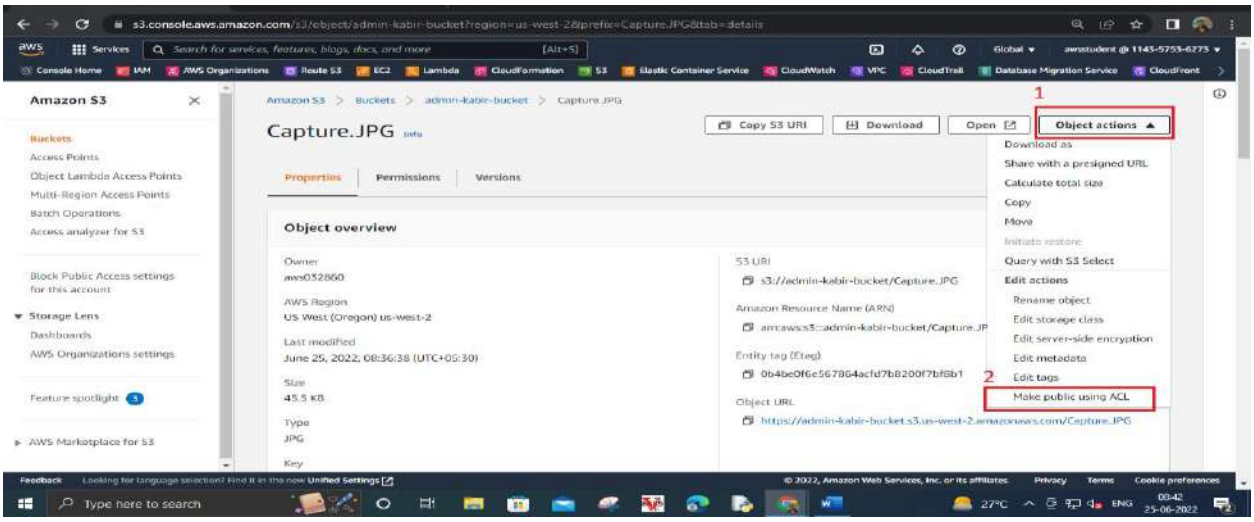
Now that you've confirmed the default security of S3 is private, you want to test how to make the object publicly accessible.

Step 15 – Keep the browser with the Access Denied error open and return to the web browser tab with the Management Console.

Step 16 – You should still be on the Object overview tab.

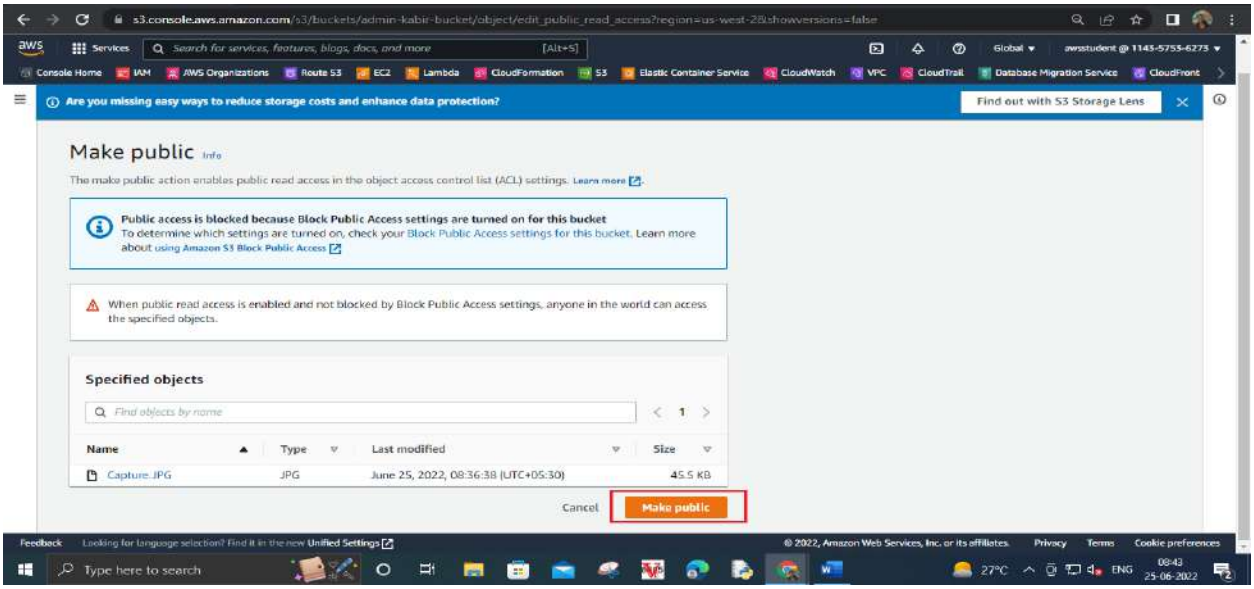
Step 17 – Close the Show Policy window.

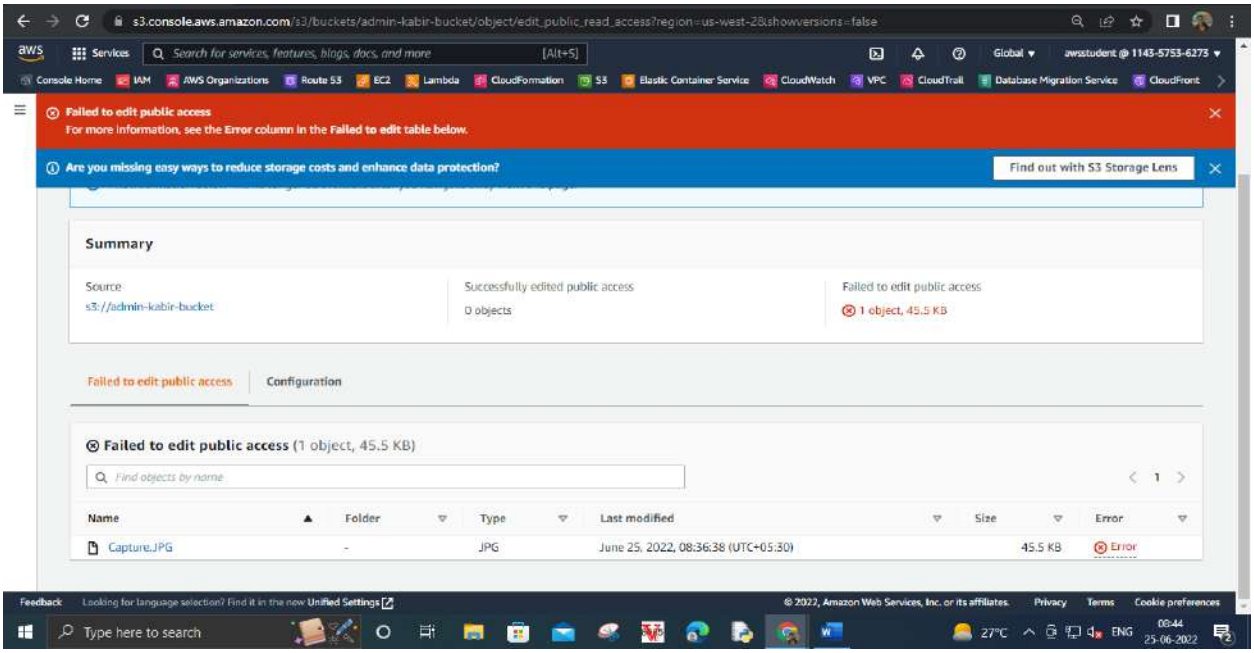
Step 18 – Choose the Object actions button and Make public via ACL. which will be the last item in the list.



Notice the warning **Public access is blocked because Block Public Access settings are turned on for this bucket**. This error displays because this bucket is configured not to allow public access. The bucket settings override any permissions applied to individual objects. If you want the object to viewable by the general public, you need to turn off Block Public Access (BPA).

Step 19 –Choose **Make Public** and read the warning at the top of the window indicating that it "Failed to edit public access" again this is due to BPA being enabled.

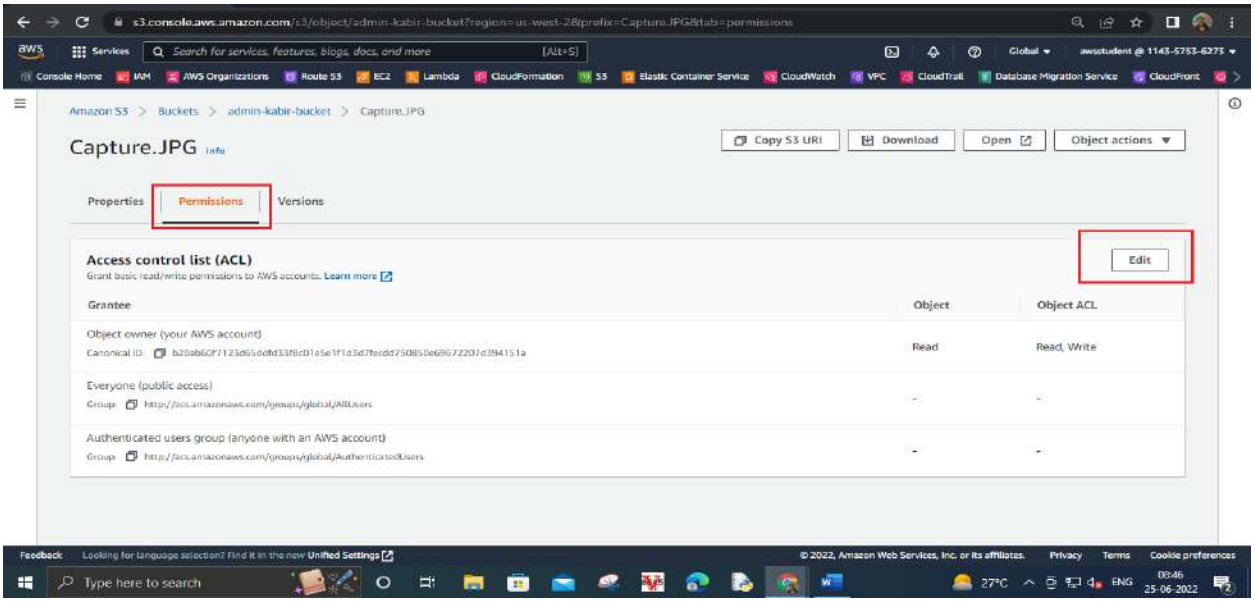




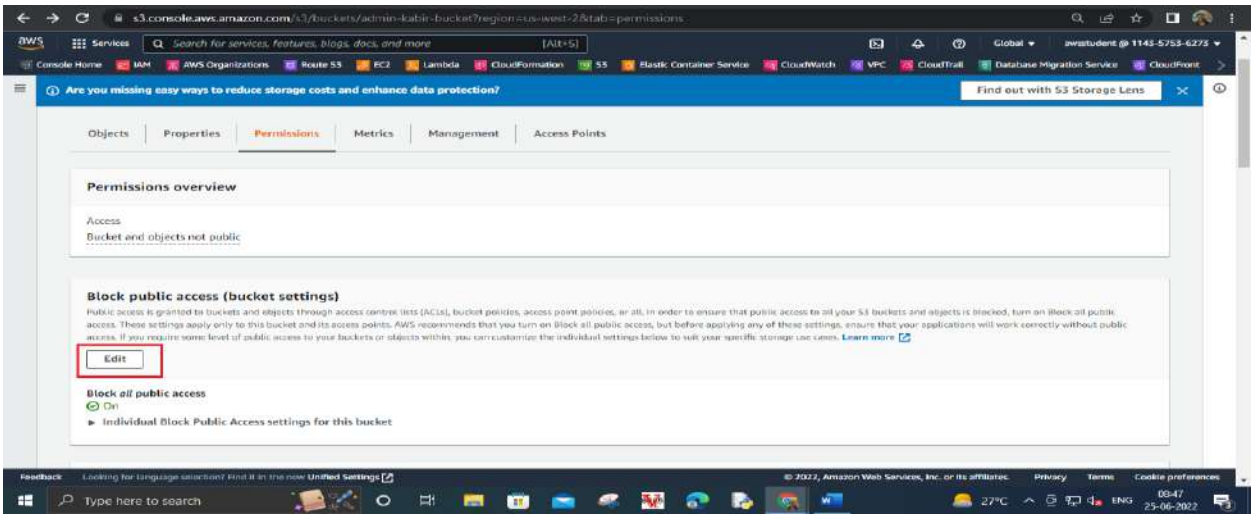
Step 20 – Choose Close to return to the object overview.

Step 21 – Use the navigation at the top to go back to the main admin-kabir-bucket overview page.

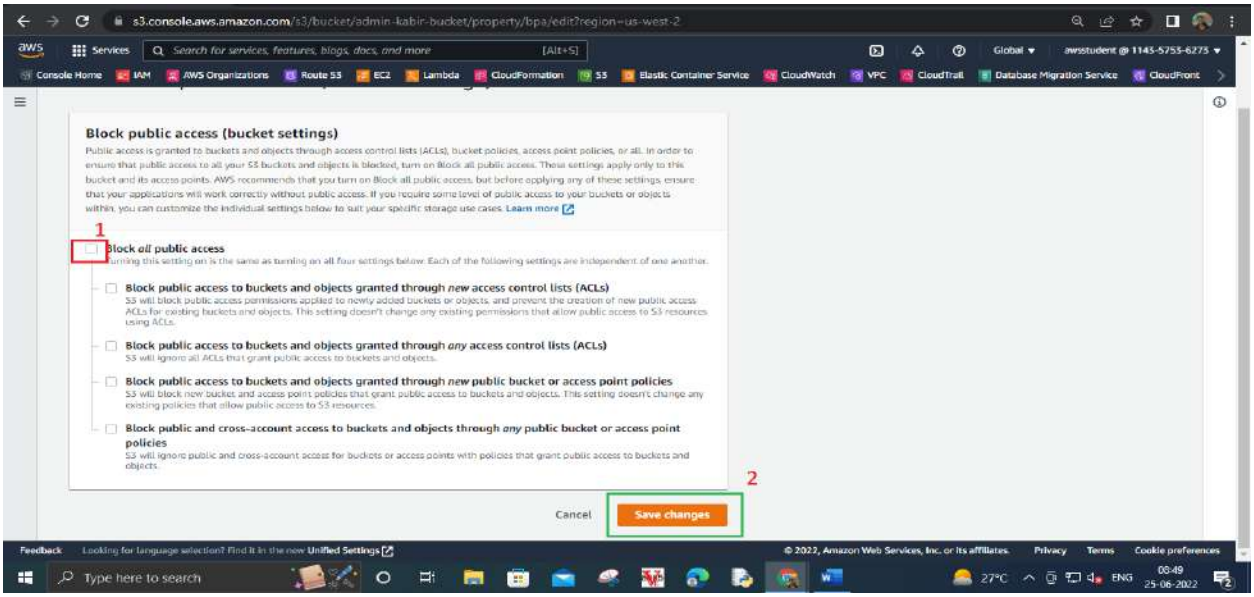
Step 22 – Choose Permission tab.



Step 23 – Under Block public access (bucket settings), choose Edit to change the settings.

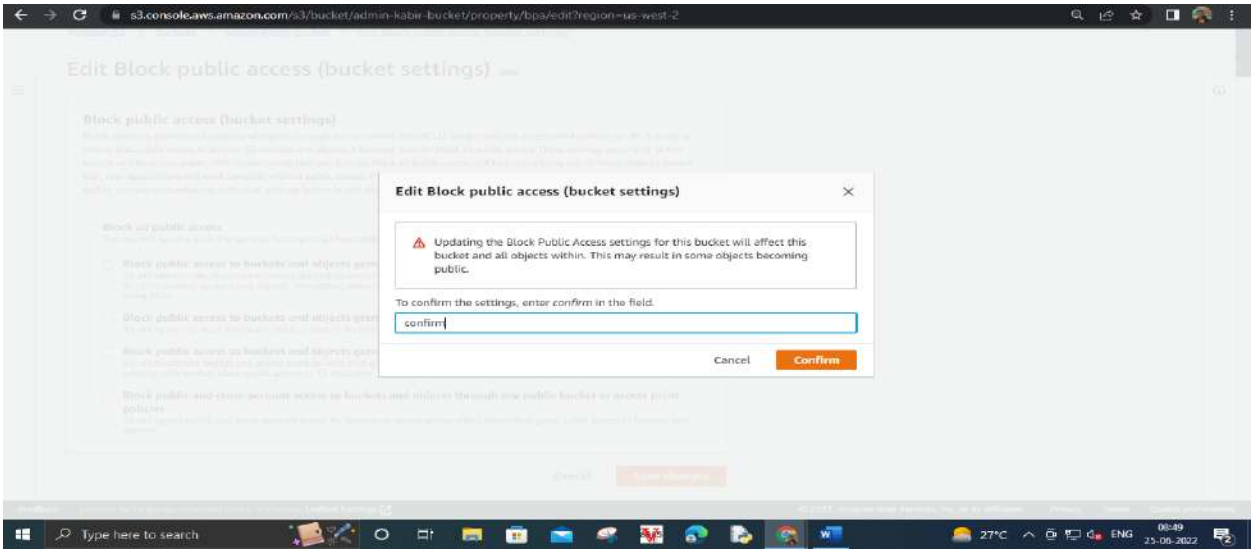


Step 23 – Deselect the Block public access option, and then leave all other options deselected.

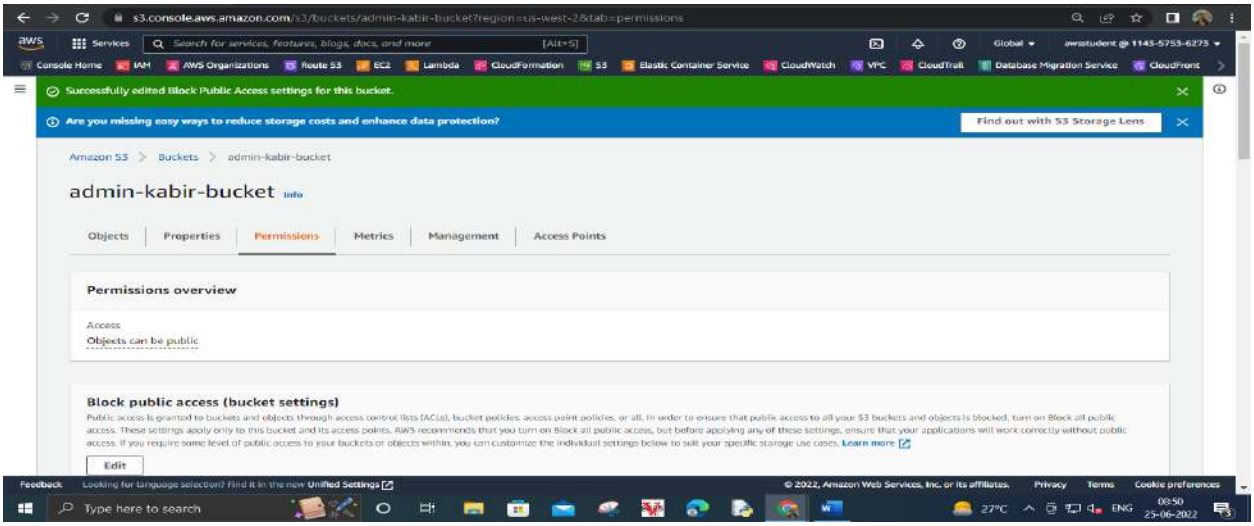


Step 24 – Choose Save Changes.

Step 25 – A dialogue box opens asking you to confirm your changes. Type confirm in the field, and then choose confirm.

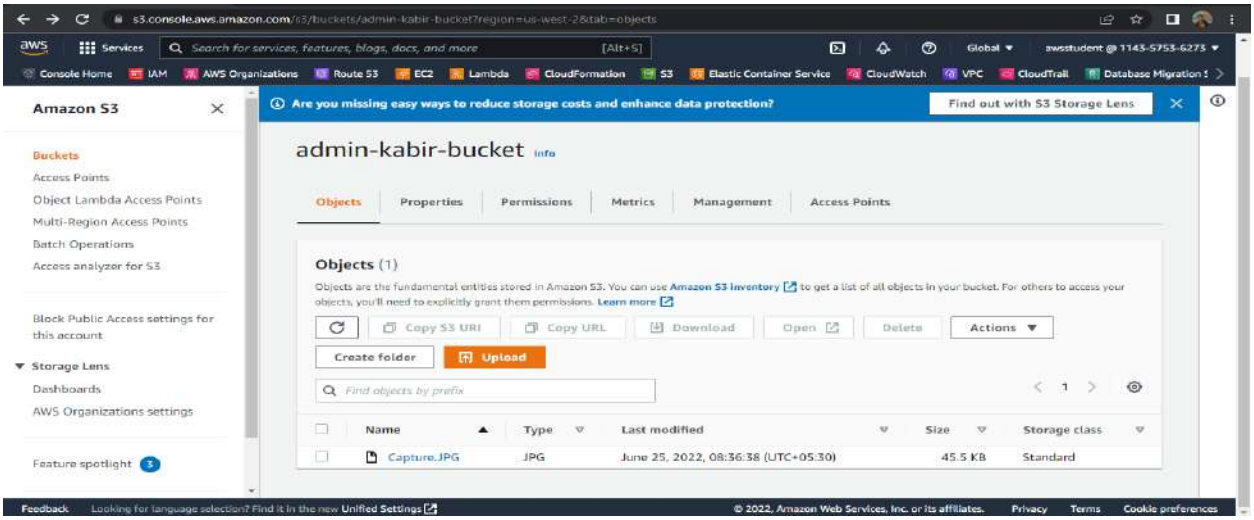


A Successfully edited bucket settings for Block Public Access message displays at the top of the window.

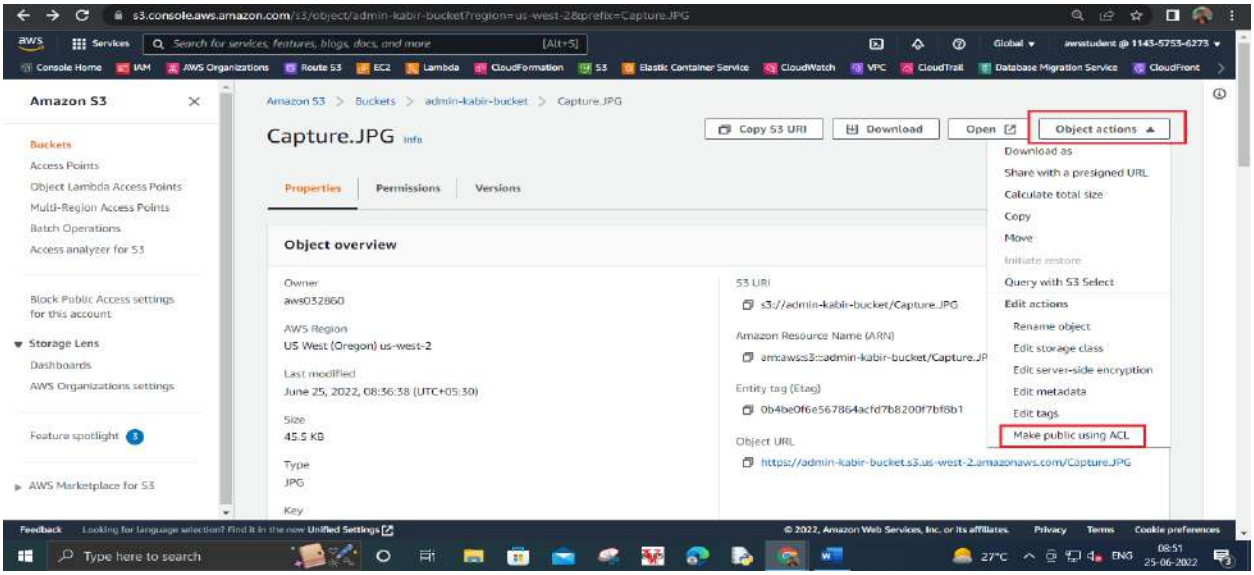


Step 26 – Choose the Objects Tab.

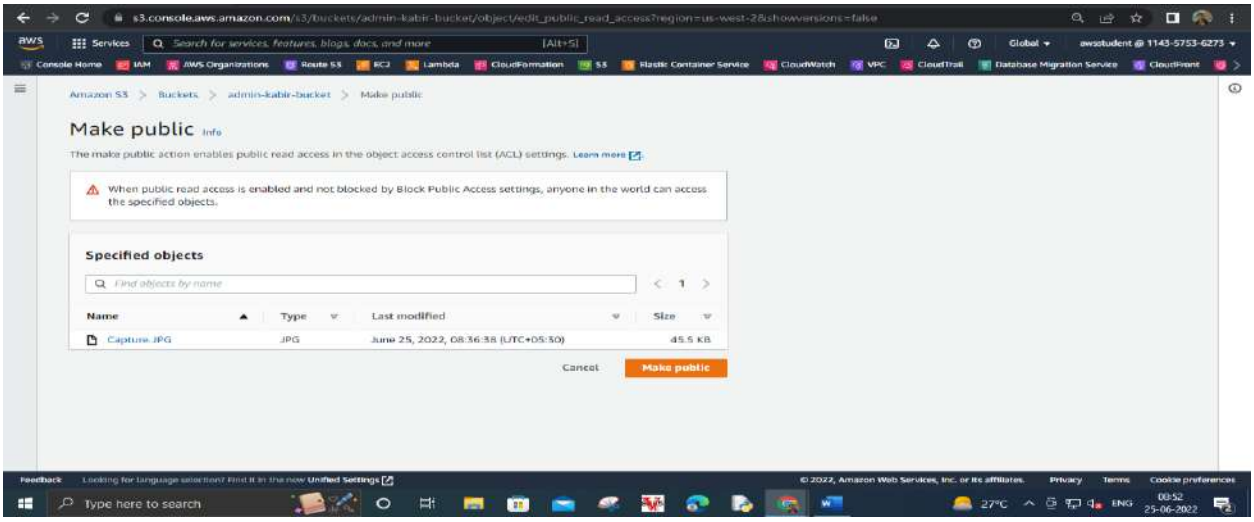
Step 27 – Choose the File name.



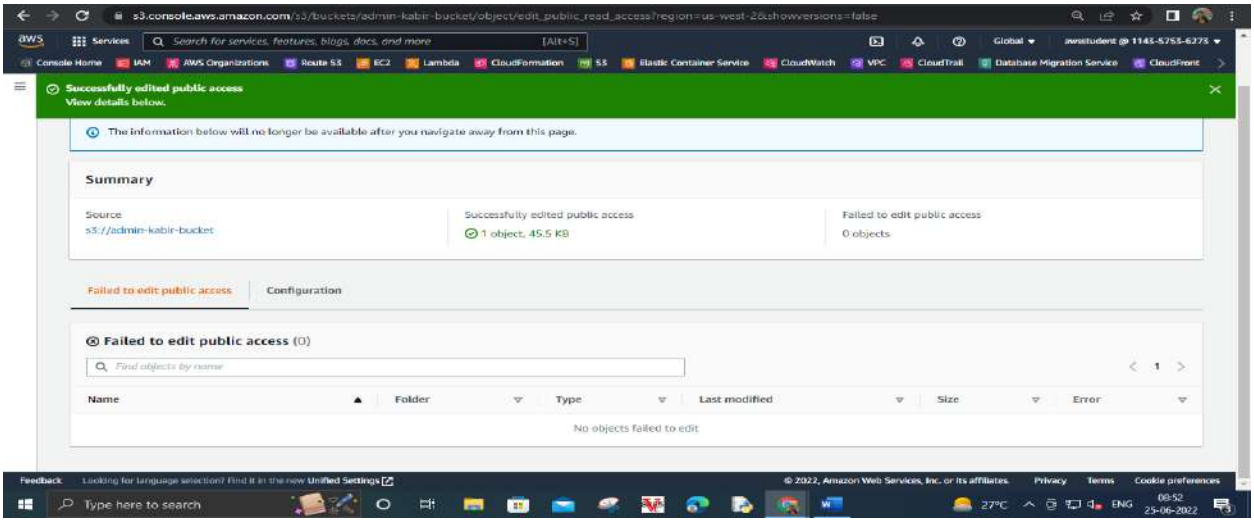
Step 27 – On the Capture.jpg overview page, choose the Object actions button and select Make public via ACL.



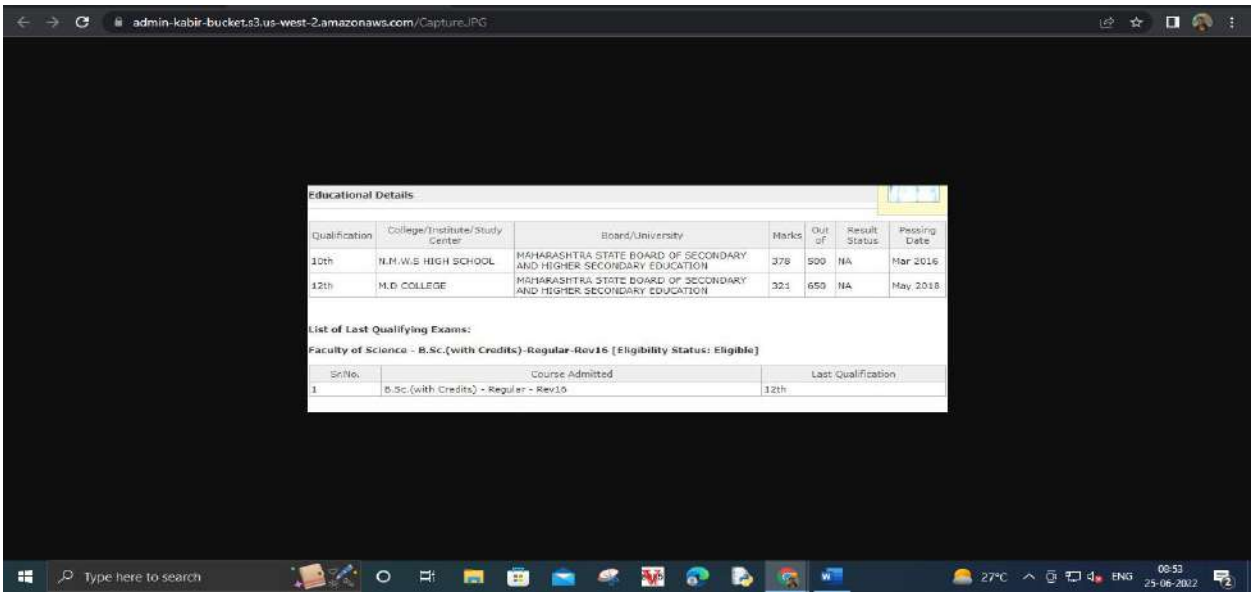
Step 28 – Choose Make public and you should see the green banner Successfully edited public access at the top of the window.



Step 29 – Choose Close to return to the object overview.



Step 30 – Return to the other browser tab that displayed Access Denied for the page and refresh.



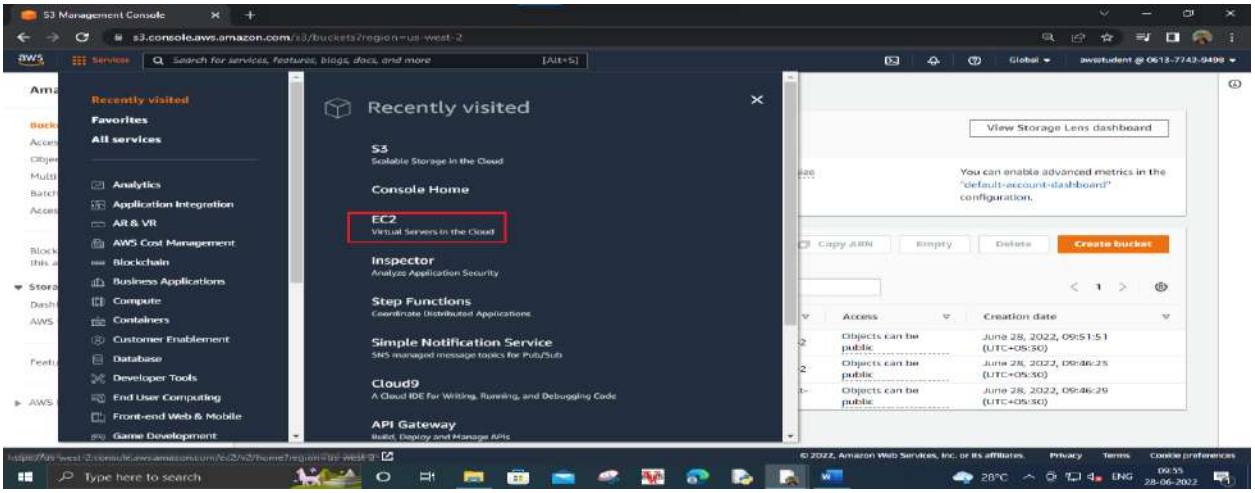
Close the web browser tab that displays your.png image and return to the tab with the Amazon S3 Management Console.

Task 4: Test connectivity from the EC2 instance

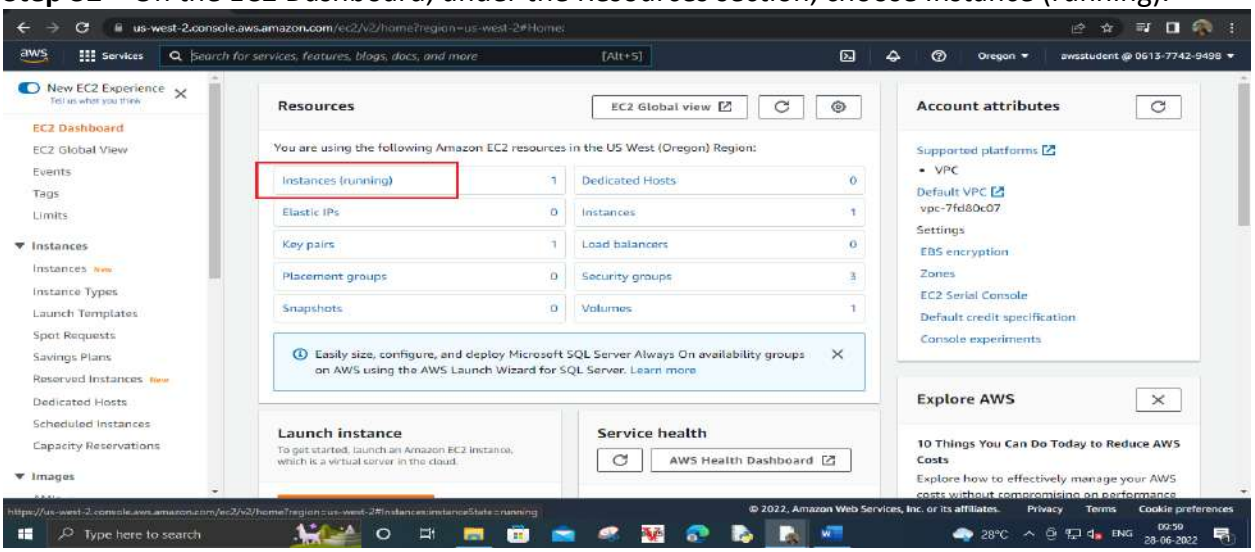
In this task, you connect to your Amazon Elastic Compute Cloud (Amazon EC2) instance to test connectivity and security to the S3 admin-kabir-bucket.

You should already be logged into the AWS Management Console. If not, follow the steps in the Start Lab section to log in to the AWS Management Console.

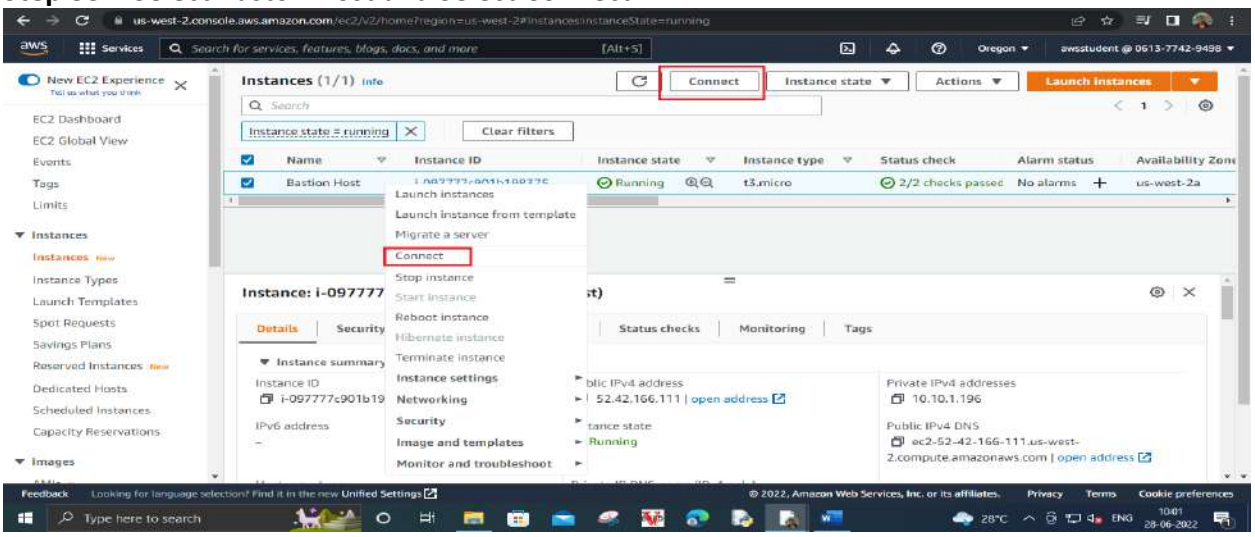
Step 31 – On the service Menu choose EC2.



Step 32 – On the EC2 Dashboard, under the Resources section, choose Instance (running).

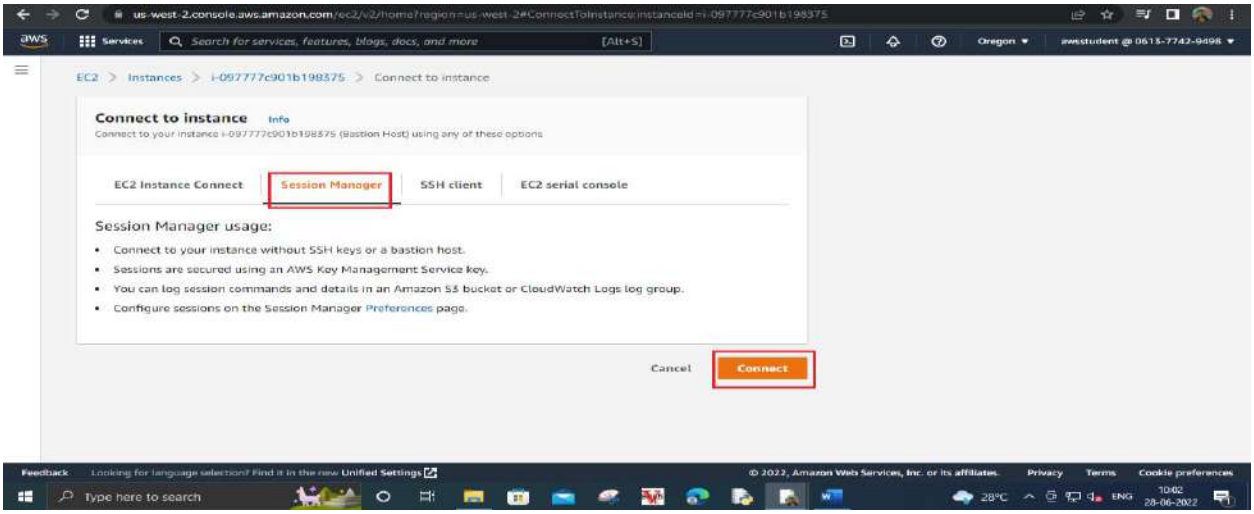


Step 33 – Select Baston Host and Select Connect.



Step 34 – In the Connect to instance window:
For Connection method, select Session Manager

Step 35 – Choose Connect.



A new browser tab or window opens with a connection to the bastion host instance.

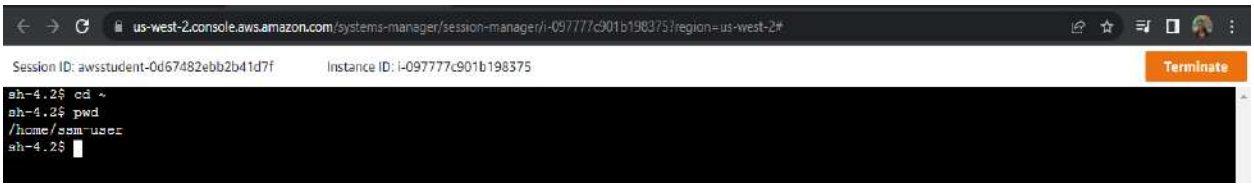
Step 36 – 34. In the bastion host session, enter the following command to change to home directory (/home/ssm-user/):

```
cd ~
```

Step 37 – Enter the following command to verify you are in the home directory.

```
pwd
```

The output should be:



You are now in the ssm-user's home directory where you will run all of the commands in this lab.

Step 38 – Enter the following command to list all of your S3 buckets.

```
aws s3 ls
```

The output should look similar to this:

You see the admin-kabir-bucket you created as well as lab auto-generated buckets.

Note: During the creating of the lab environment, both an Instance Profile (which defines who you are for authentication) and a Role (which defines what you can do after you authenticate), have been automatically added for the EC2 instance to allow the EC2 instance to list the S3 buckets and objects.

Step 39 – Enter the following command to list all objects in your admin-kabir-bucket. Remember to change the number at the end of the admin-kabir-bucket name, to match the name of the bucket you created.

```
aws s3 ls s3://admin-kabir-bucket
```

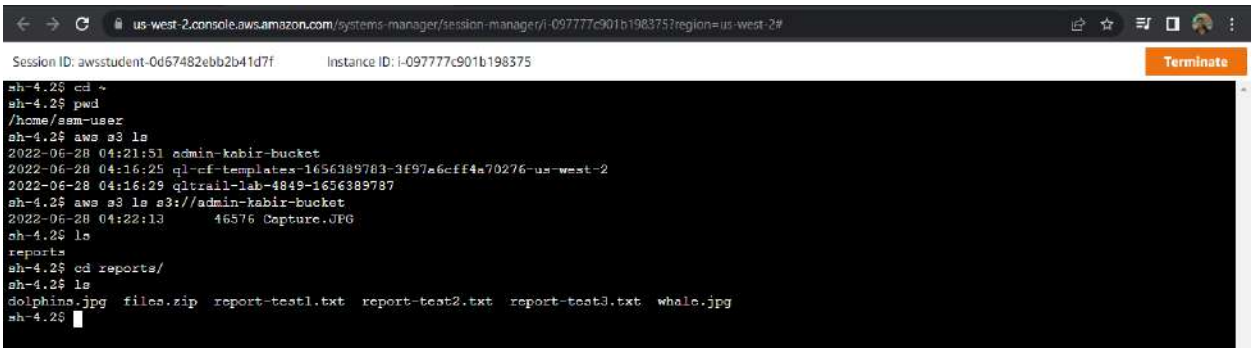
The output should look like this:

Step 40 – Type the following to change directories into the report's directory.

```
cd reports
```

Step 41 – Type the following to list the contents of the directory.

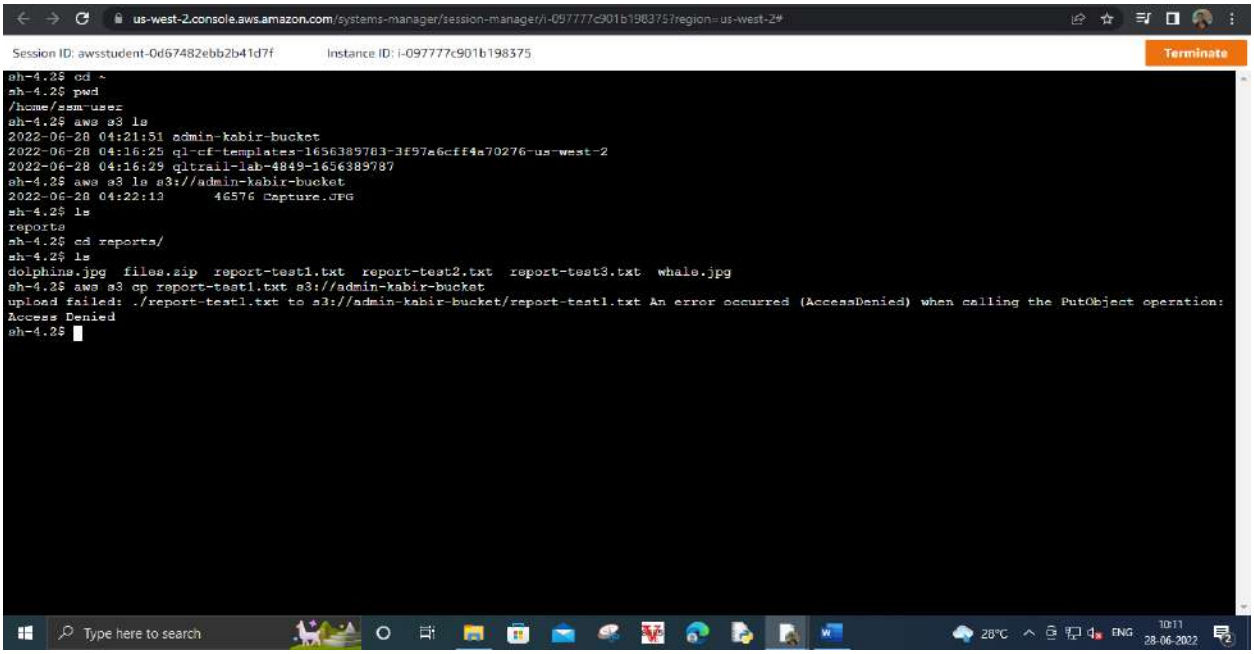
```
ls
```



Step 42 – The output shows some files created in your reports directory to test the application.

Step 43 – Type the following to see if you can copy a file to the S3 bucket.

```
aws s3 cp report-test1.txt s3://admin-kabir-bucket
```



The output indicates an error upload failed. This is because we have read-only rights to the bucket and do not have the permissions to perform the Put Object operation.

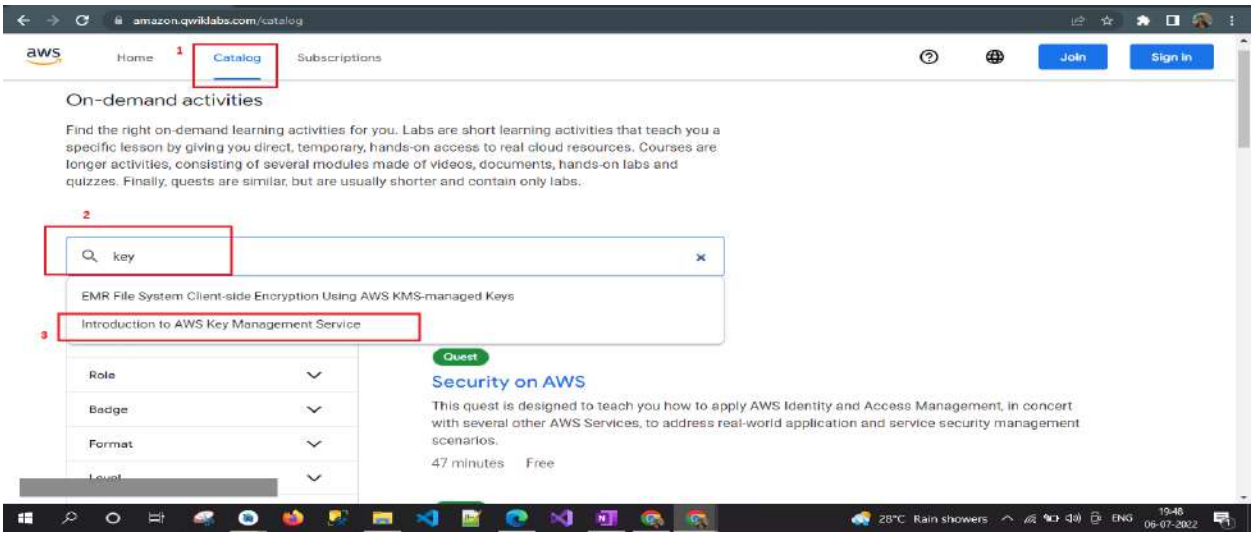
Leave this window open and go back to the AWS Console tab.

Practical 4: Introduction to AWS Key management Service

A. Create KMS master key
B. Configure CloudTrail to store Logs in an S3 Bucket
C. Upload an Image to S3 bucket and encrypt it
D. Access the encrypted image
E. Monitor KMS activity Using CloudTrail Logs
F. Manage encryption keys

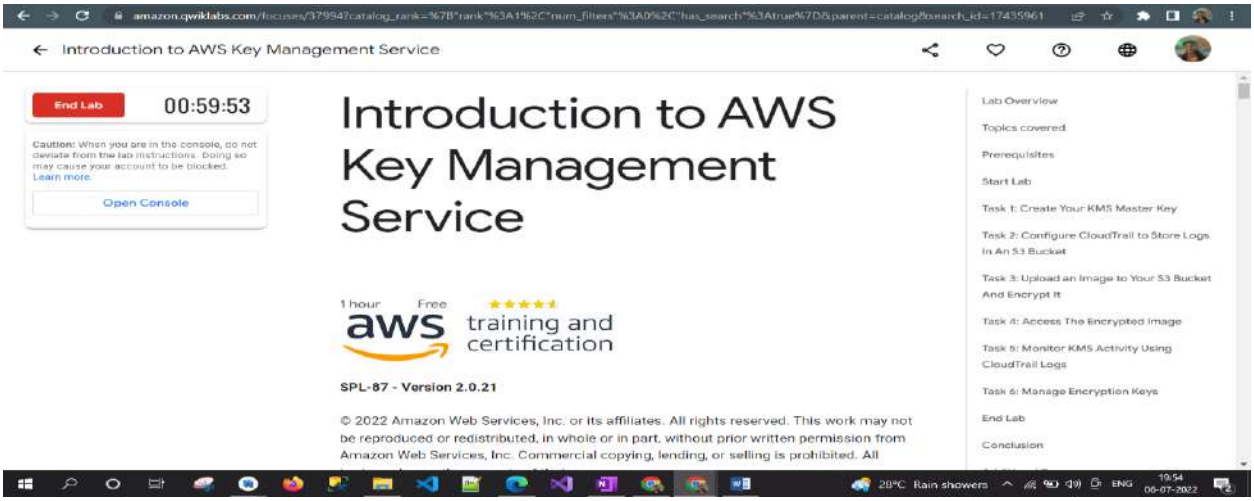
Task 1: Create Your KMS Master Key

Note: Go to the given link https://amazon.qwiklabs.com/. After that click on the Catalog option and search the "**key**" word into the search box then show the "**Introduction to AWS Key Management Service**" option. Click on that option.

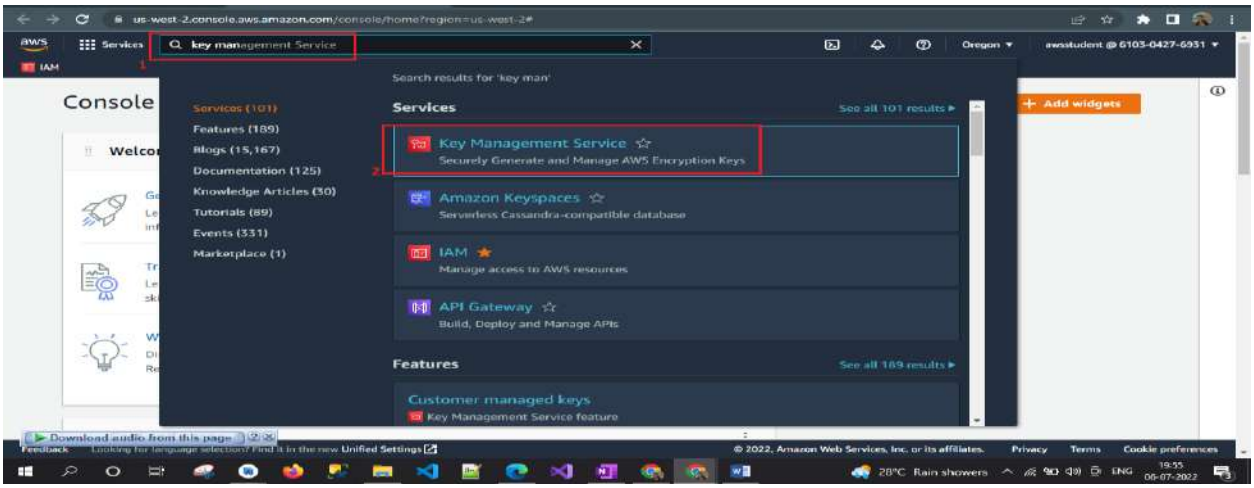


Step 1 – At the top of your screen, launch your lab by choosing click on the **Start Lab** button and wait for few seconds

Step 2 – Open your lab by click on the **Open Console** button

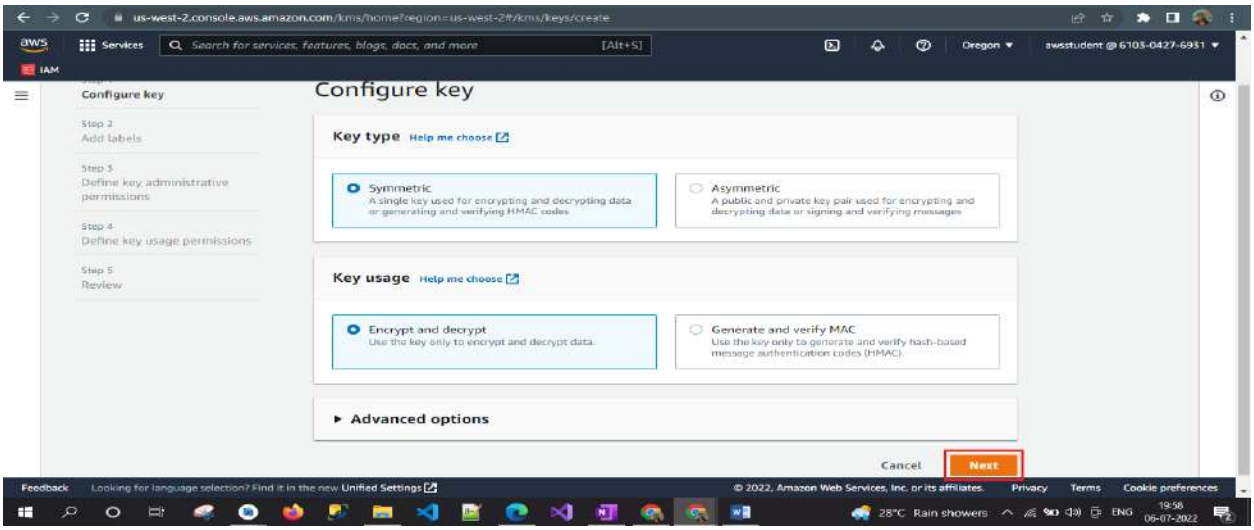


Step 3 – In the **AWS Management Console**, on the Service menu, click **Key Management Service**.



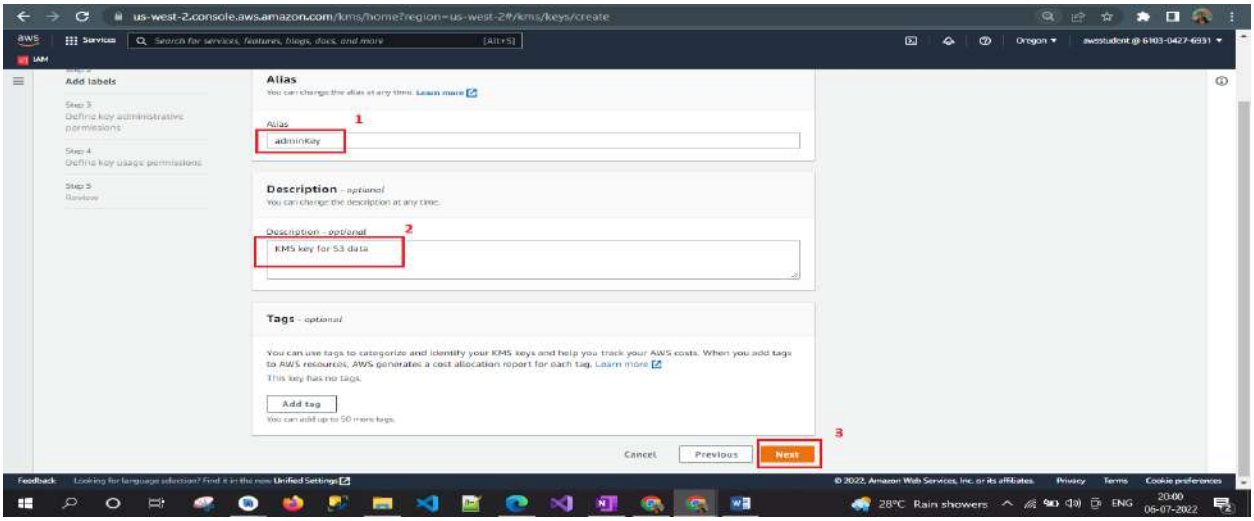
Step 4 – Click Create a key the configure:

- On the Configure Key page Key type -> Select **Symmetric** Key usage -> Select **Encrypt and decrypt**
- Click **Next**



Step 5 – On the Add Labels page configure:

- **Alias**: adminKey
- **Description**: KMS Key for S3 Data
- **Click**: Next



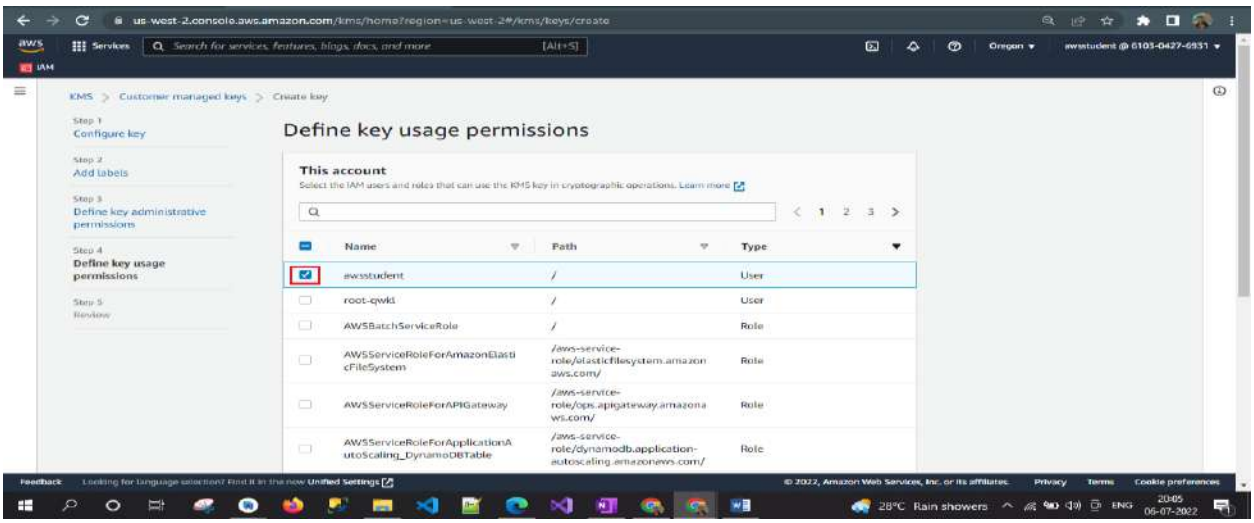
It is a good practice to describe what services the encryption key will be associated within the description.

Step 6 – On the **Define Key administrative permission**, select the user or role you are signed into the console with.

The user is displayed at the top of the page, to the right of the region.

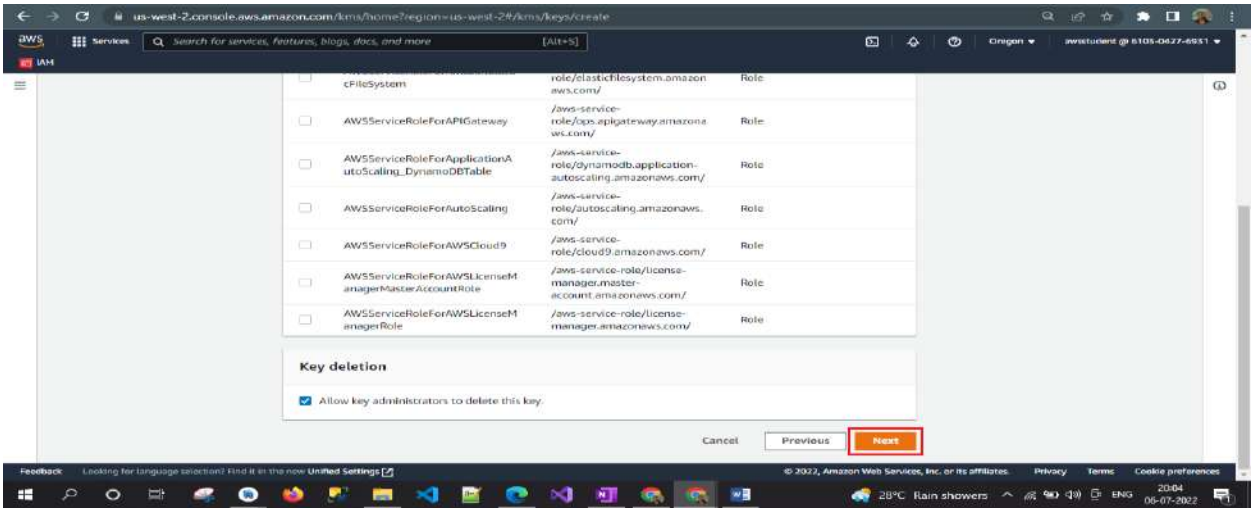
Step 7 – Next.

Step 8 – On the **Define Key usage permission** page, select the user or role you are signed into the console with.



Step 9 – Next.

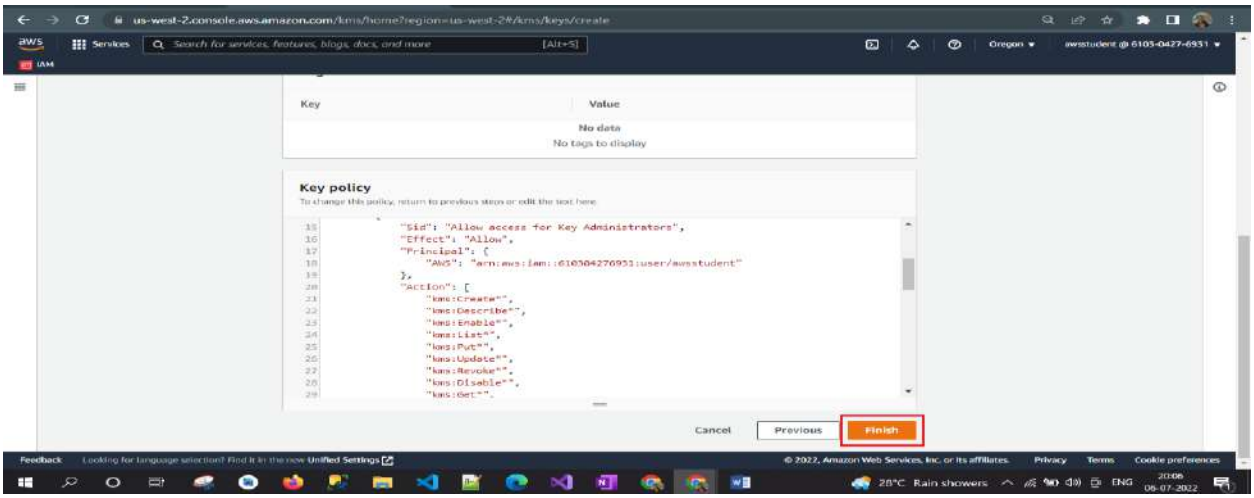
Key Users are the users or role that will use the key to encrypt and decrypt data.



Step 10 – On the **Review and edit key policy** page:

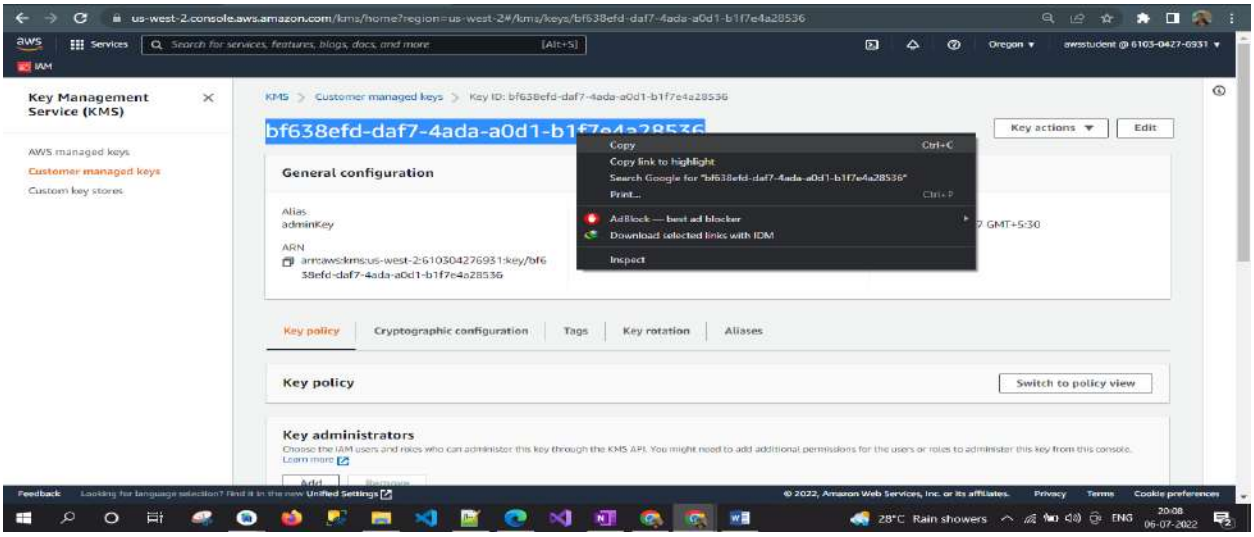
- Review the key policy

- Click Finish.



Step 11 – Copy the Key ID for adminKey to a text editor.

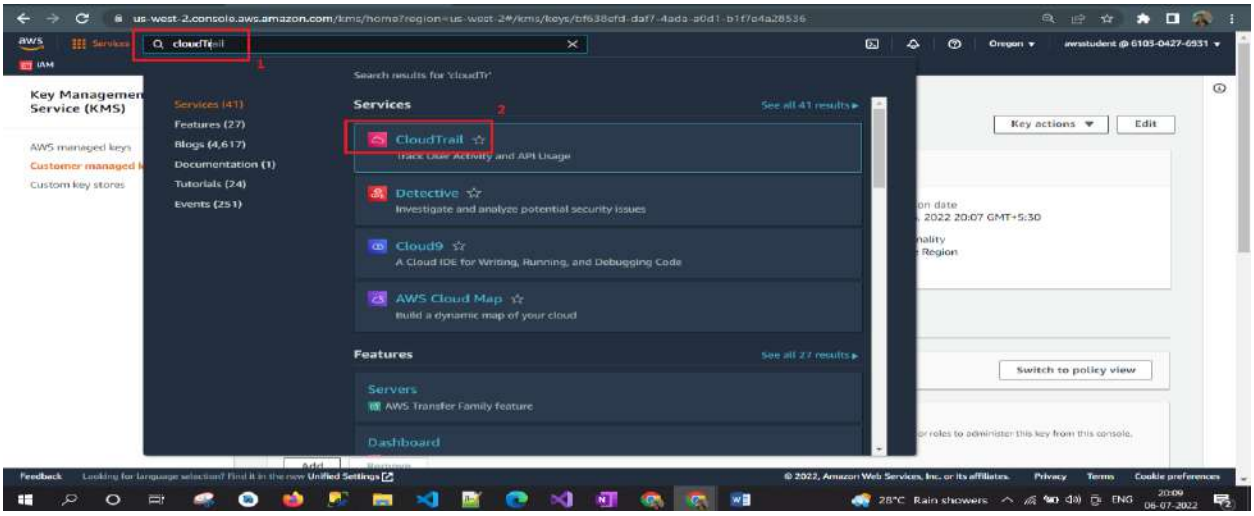
You will use this key id later when looking at the Log activities for this KMS key.



Task 2: Configure Cloud trail to store logs in an S3 bucket

In this task you will configure cloud trail to store log files in a new S3 bucket.

Step 12 – On the Service menu, click CloudTrail.

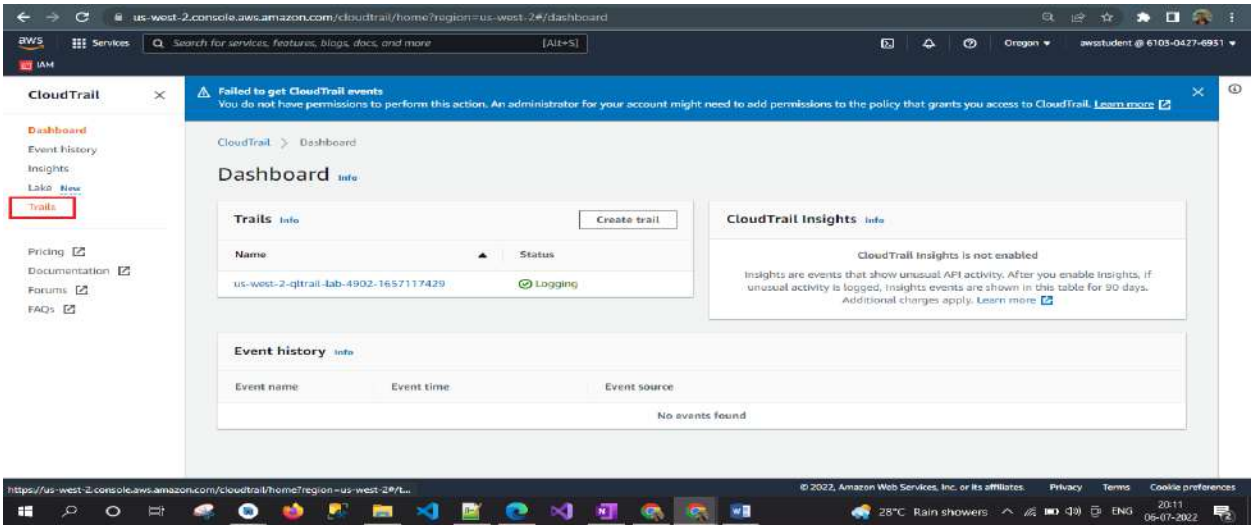


Step 13 – If you see the New Event history features available in the new Cloud trail console with Try Out the new console, click try out the new console, otherwise you can ignore this warning.

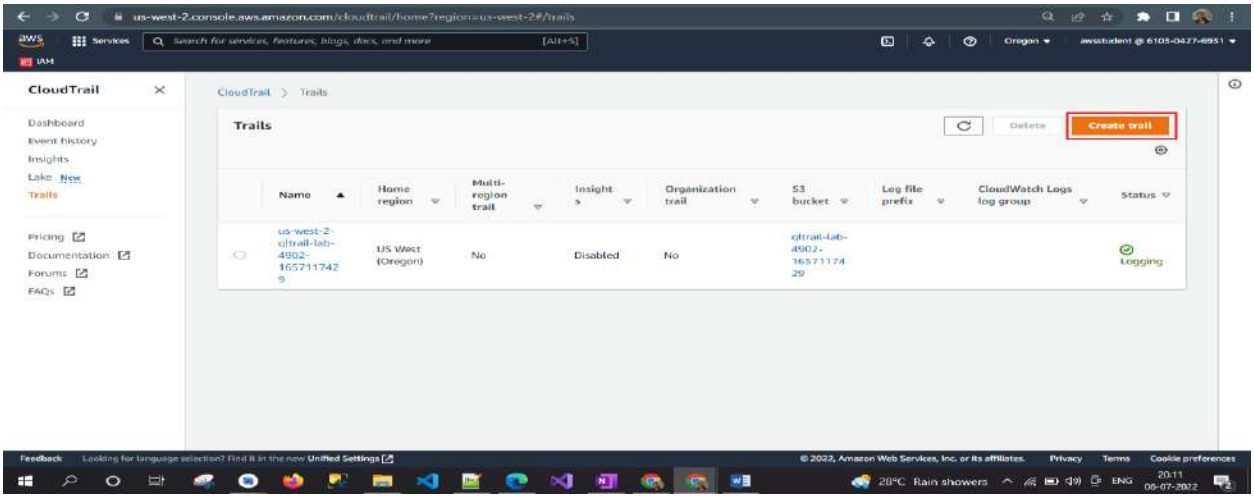
Step 14 – If you see a warning saying the option to create an organization trail is not available for this AWS account, you can ignore this warning.

Step 15 – If you see You do not have permission to perform this action. An administrator for your account might need to add permission to the policy that grant you access to Cloud Trial, you can ignore this warning.

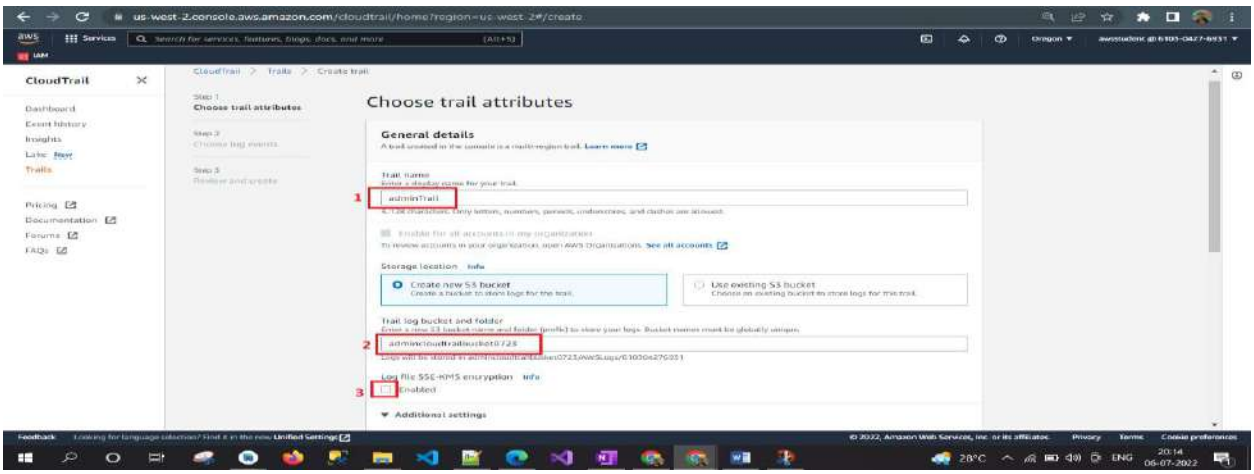
Step 16 – In the navigation pane on the left, click Trails.



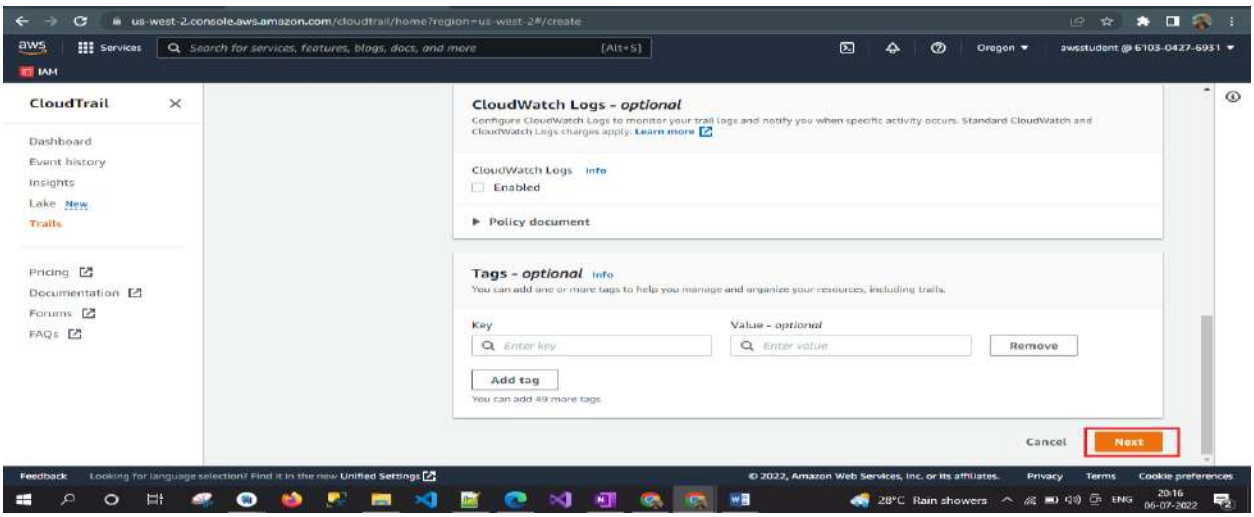
Step 17 – Click Create trail then configure:



- **Trail name:** adminTrail
- **Trail log bucket and folder:** admincloudtrailbucket0723
- Replace **NUMBER** with a random number
- De-Select **Enabled** for **Log file SSE-KMS encryption**.

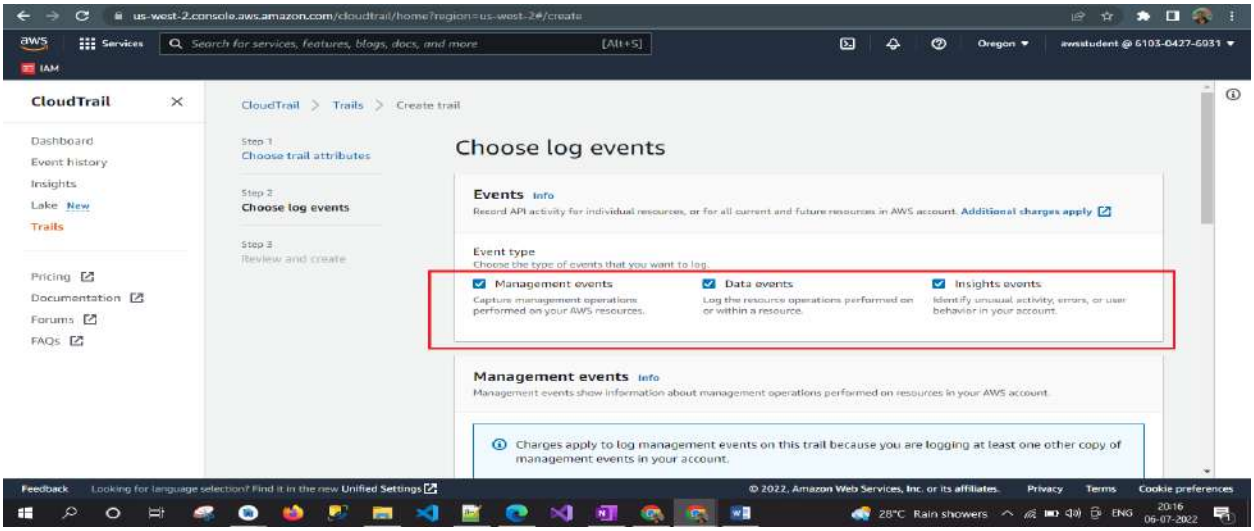


Step 18 – Click Next.

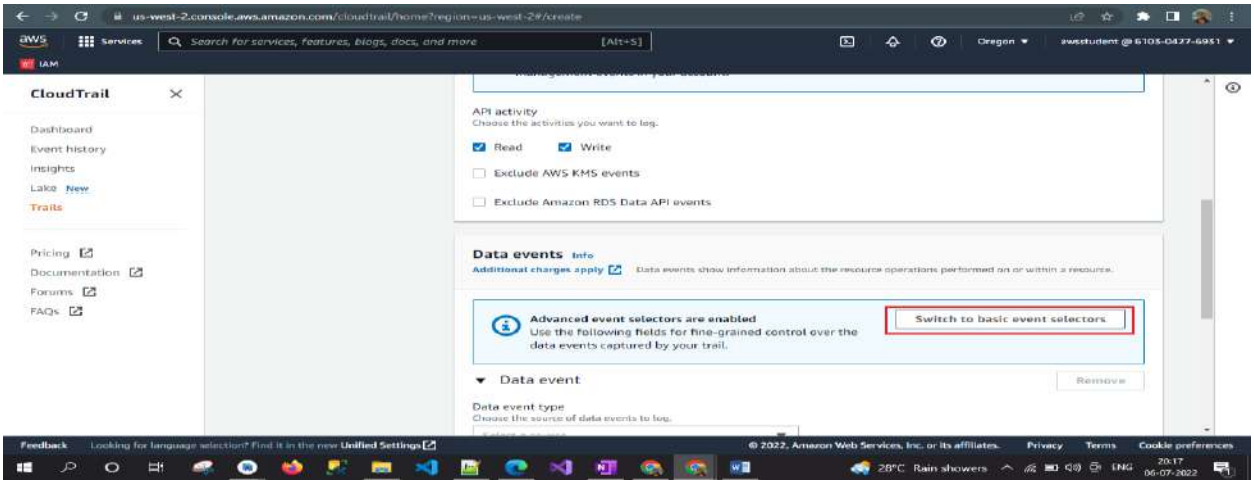


Step 19 – On the Choose Log events page, configure:

- ✓ Management event
- ✓ Data Events
- ✓ Insights events

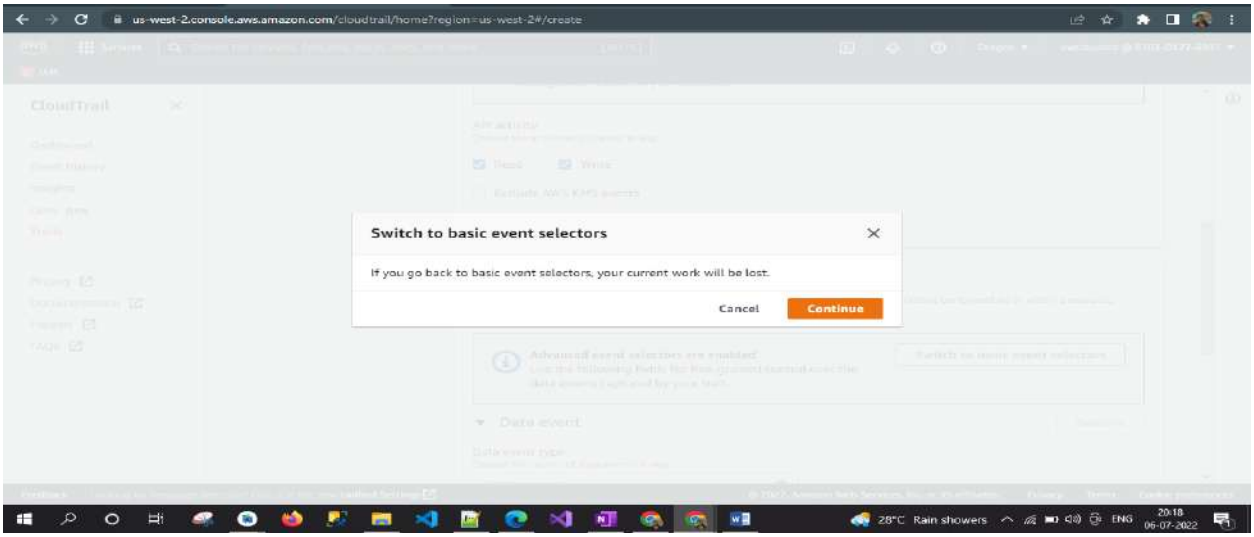


Step 20 – In the **Data events**, Select **Switch to basic event selector**.

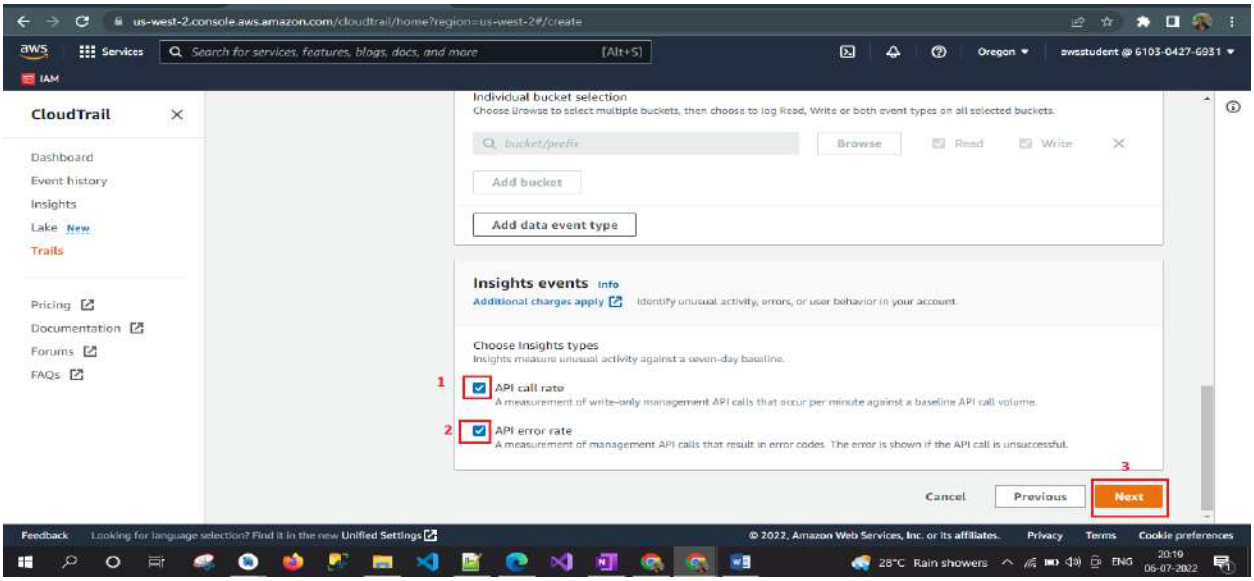


Step 21 – In the Insight event, Select

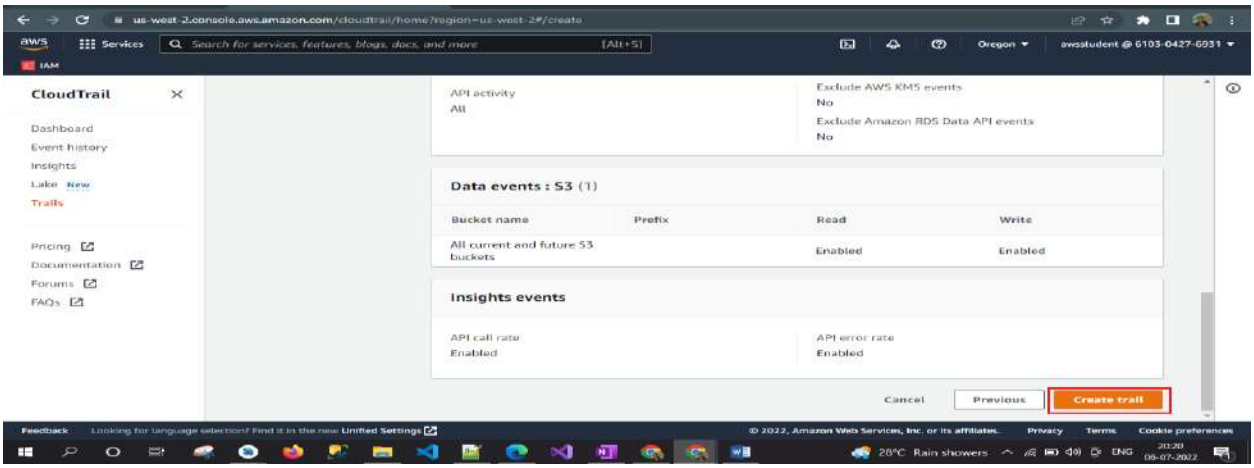
- ✓ API call rate
- ✓ API error rate



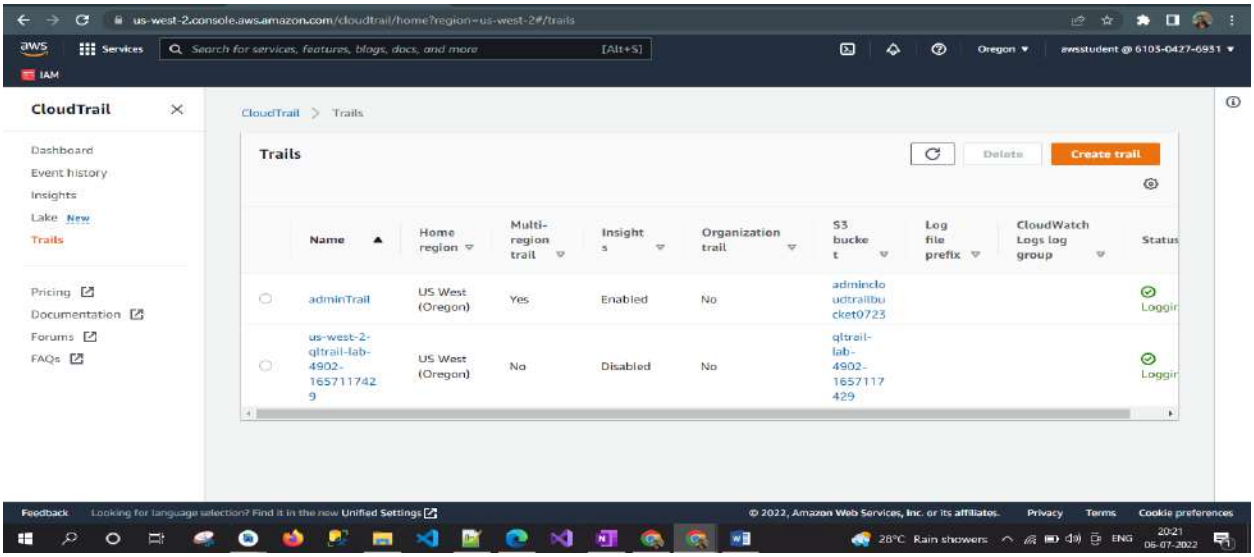
Step 22 – Click Next.



Step 23 – Click Create trail.



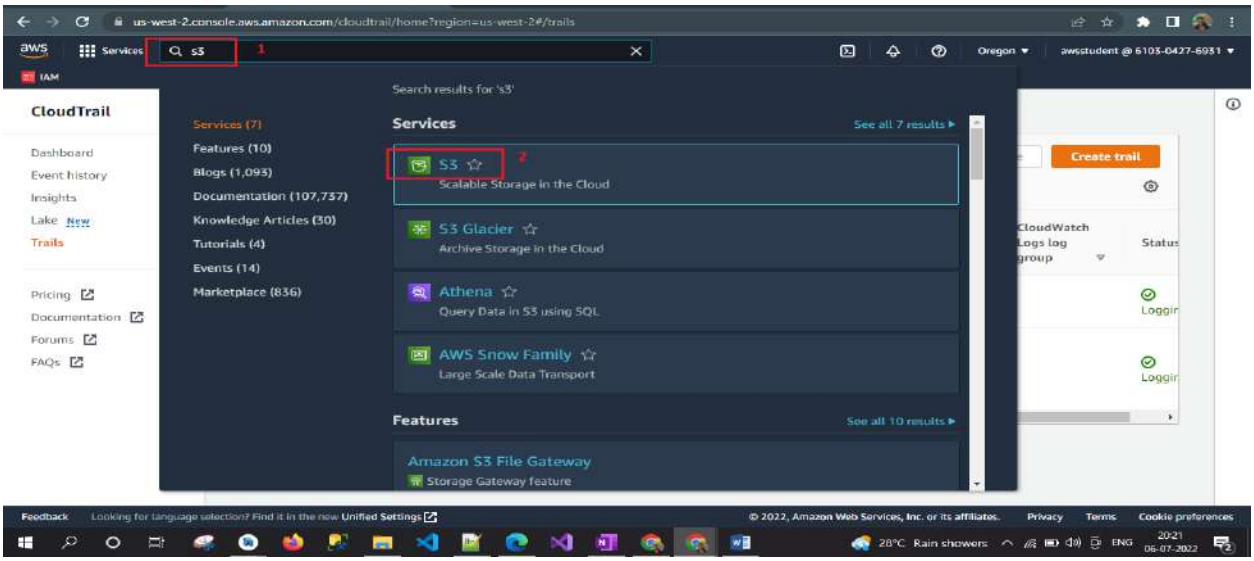
Here show the recently created the Trails i.e. **adminTrail**



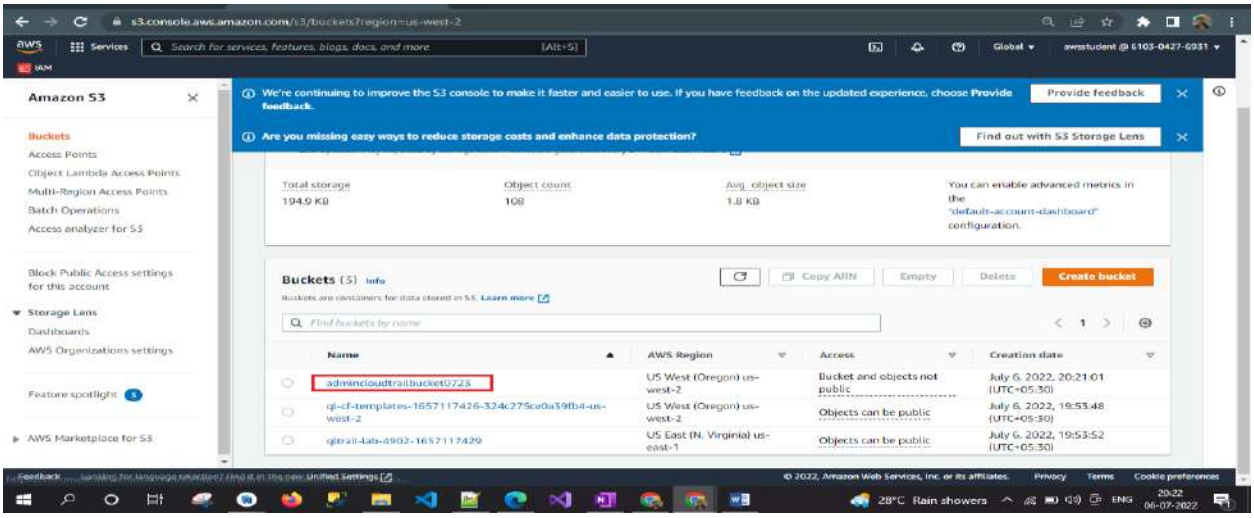
Task 3: Upload an image to your S3 bucket and Encrypt It

In this task, you will upload an image file to your S3 bucket and encrypt it using the encryption it using the encryption key you created earlier. You will use the S3 bucket you created in the previous task to store the image file.

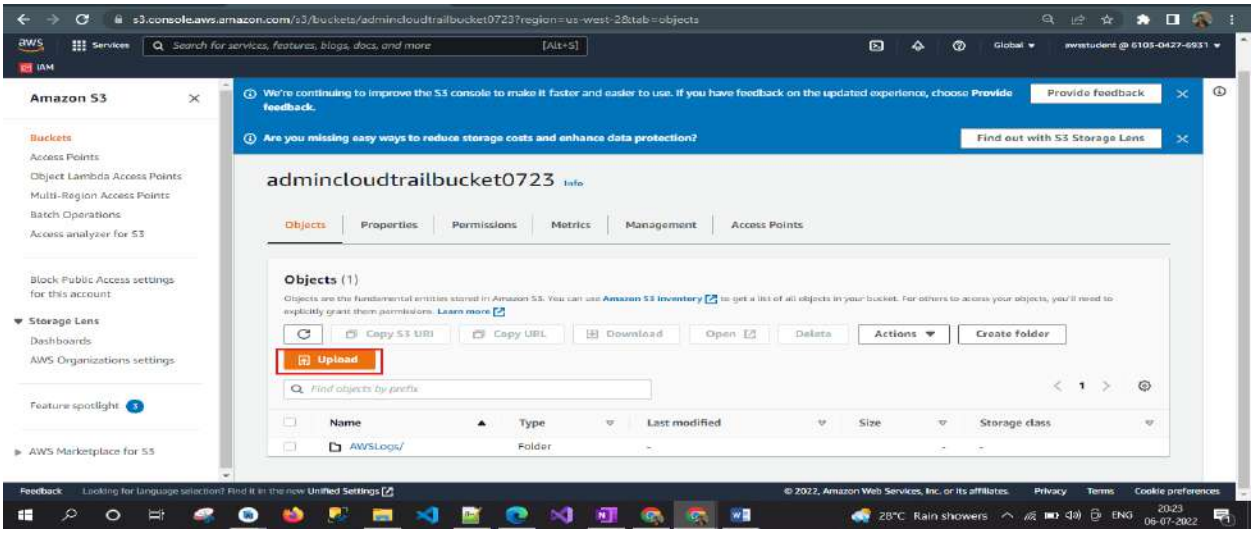
Step 24 – On the Service Menu, click S3.



Step 25 – Click **admincloudtrailbucket0723**.

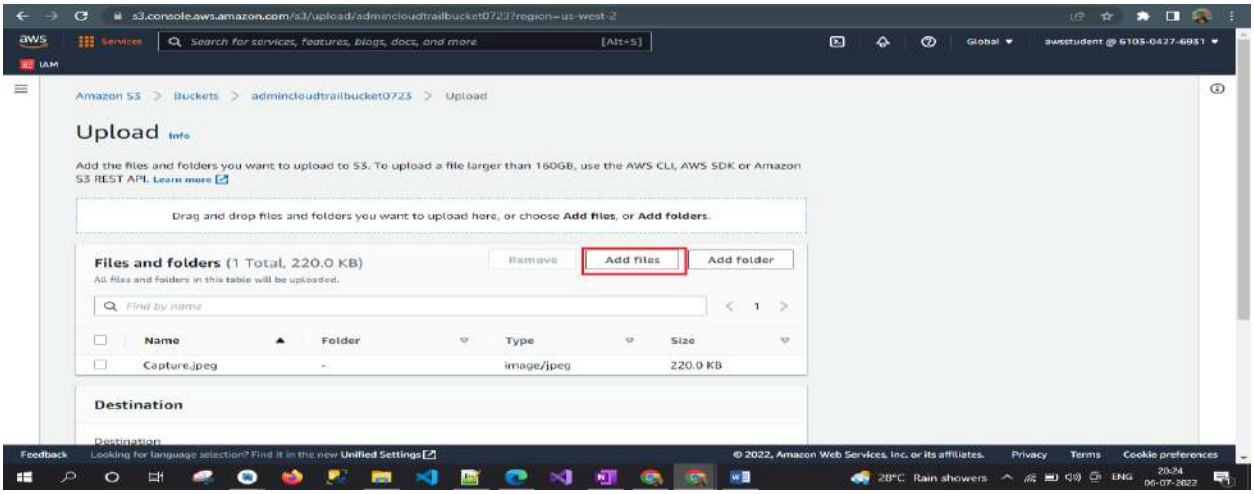


Step 26 – From the objects tab, click **Upload**.

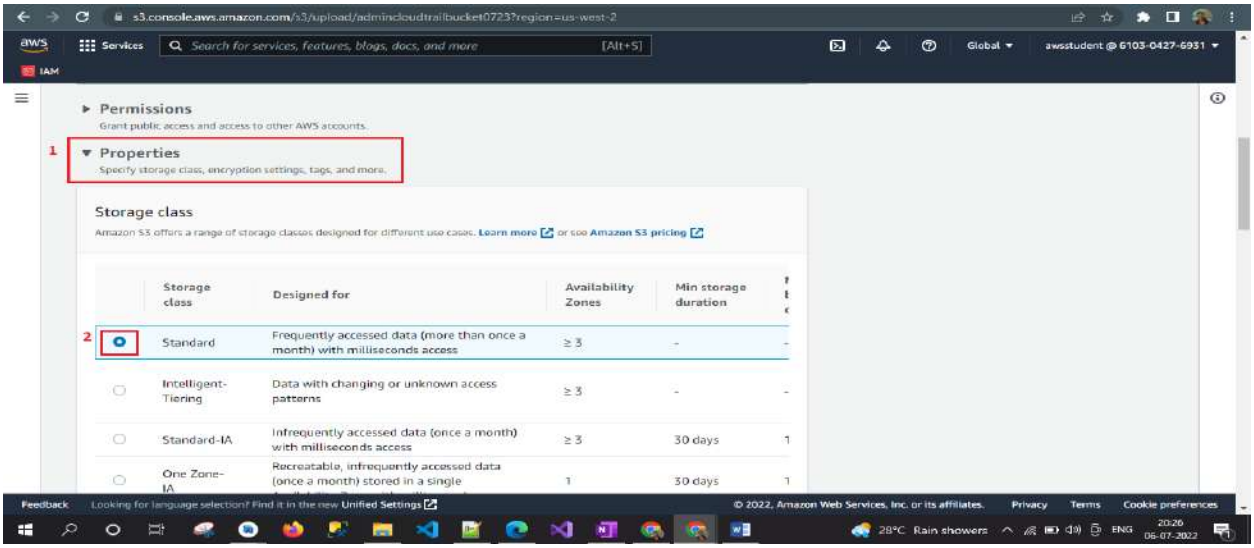


Step 27 – Click Add files.

Step 28 – browse to and select an image file on your computer.



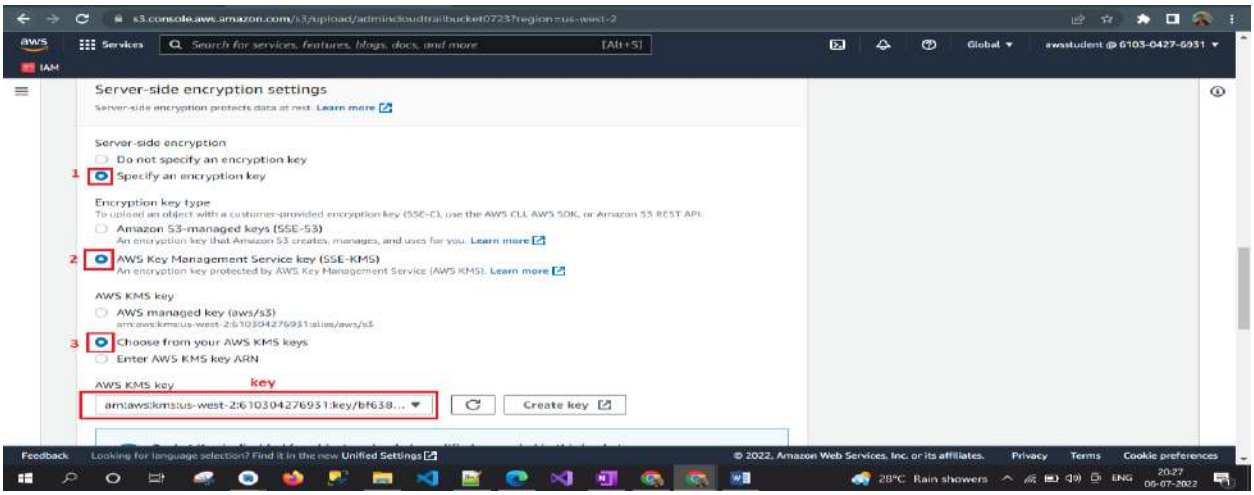
Step 29 – At the bottom of the screen expand > **Properties**.



Step 30 – In the **Server-side encryption setting** section, Select Specify an encryption Key.

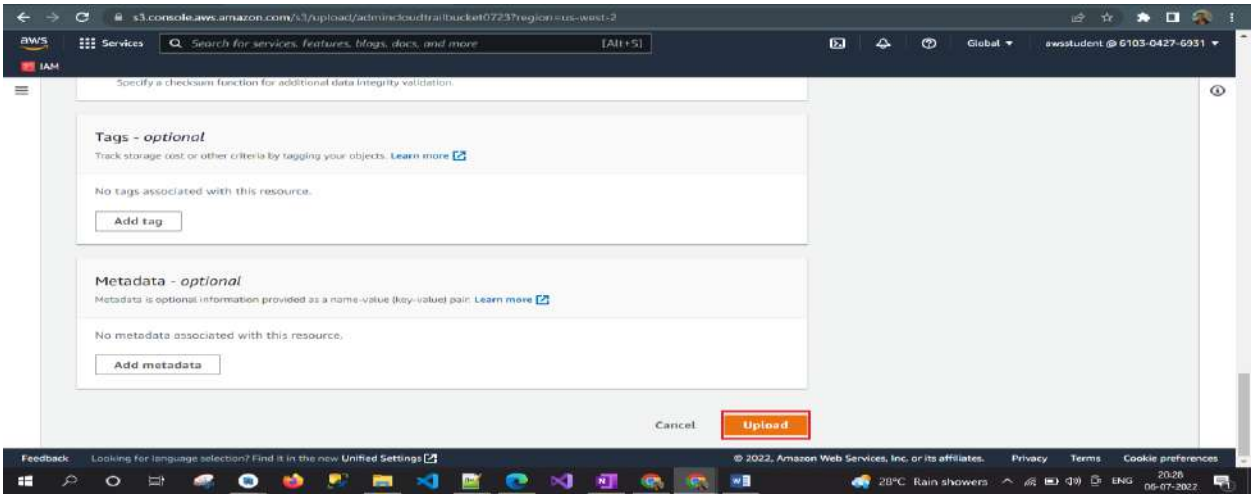
Step 31 – For **Encryption Key Type**, Select AWS Management Service Key (SSE- KMS).

Step 32 – For **AWS KMS Key** select Choose from your AWS KMS keys.

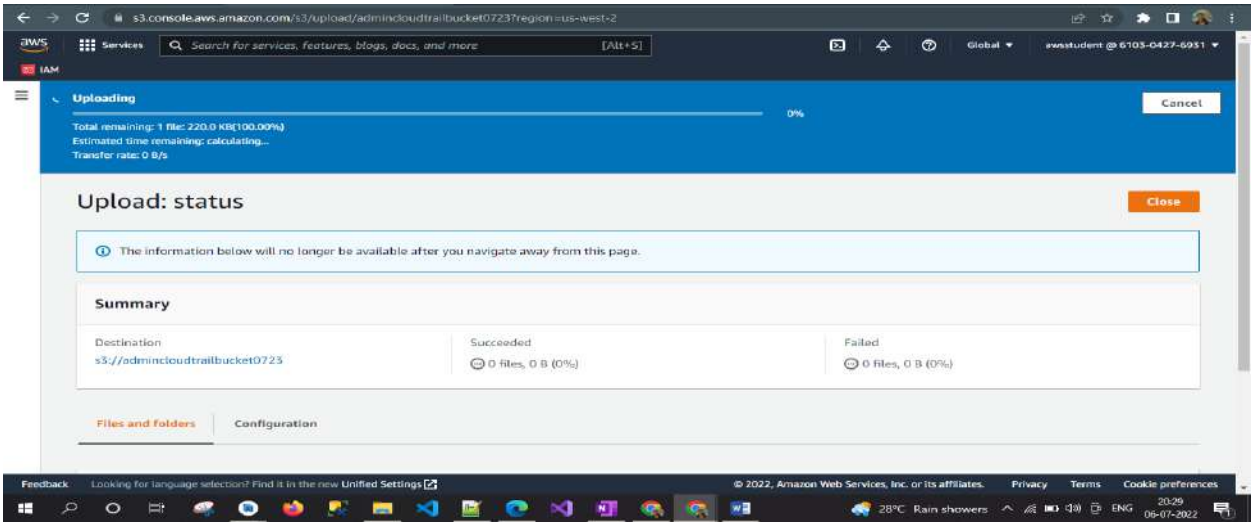


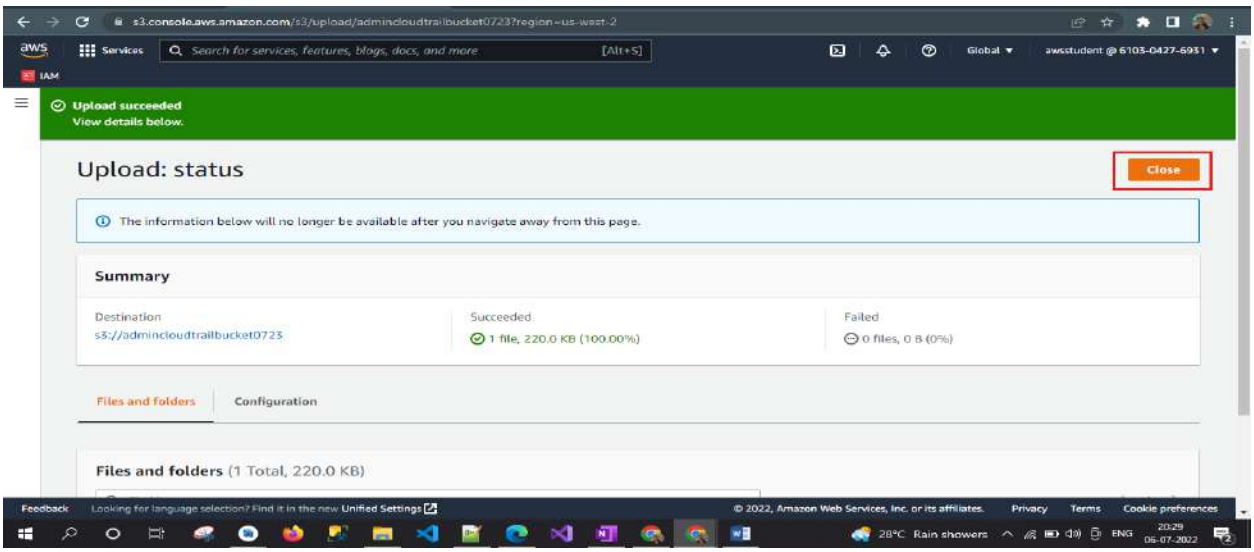
Step 33 – Form the drop down of the KMS Master key, select *adminKey*

Step 34 – Scroll to the bottom of the screen, then click Upload.



Step 35 – Click close from the right corner of the upload: status page.





Step 36 – Return to the bucket details by clicking the bucket name.

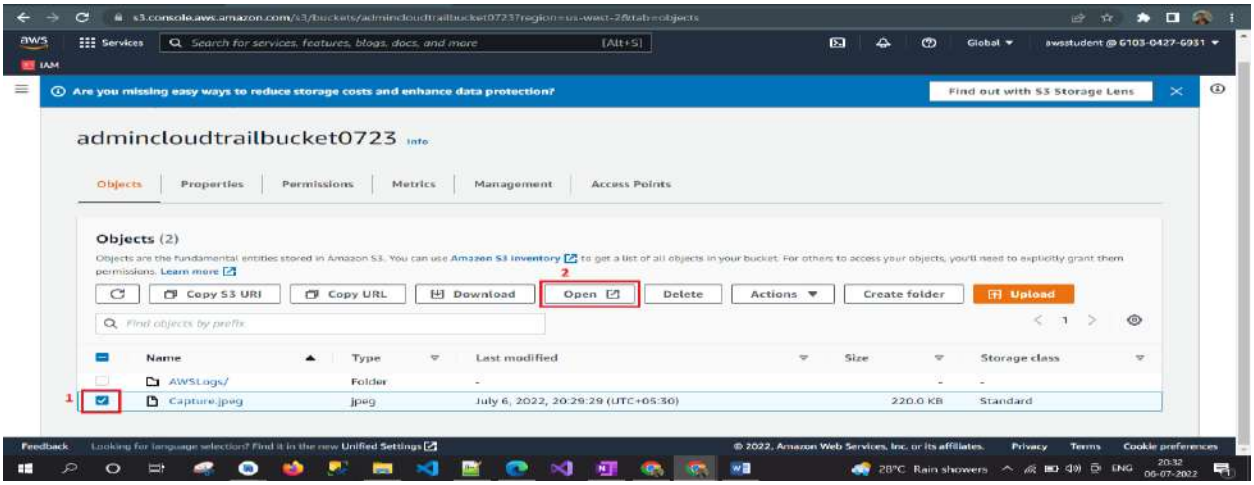
Step 37 – Record the **Last Modified** time to your text editor.

Step 38 – Return to the bucket details by clicking the bucket name.

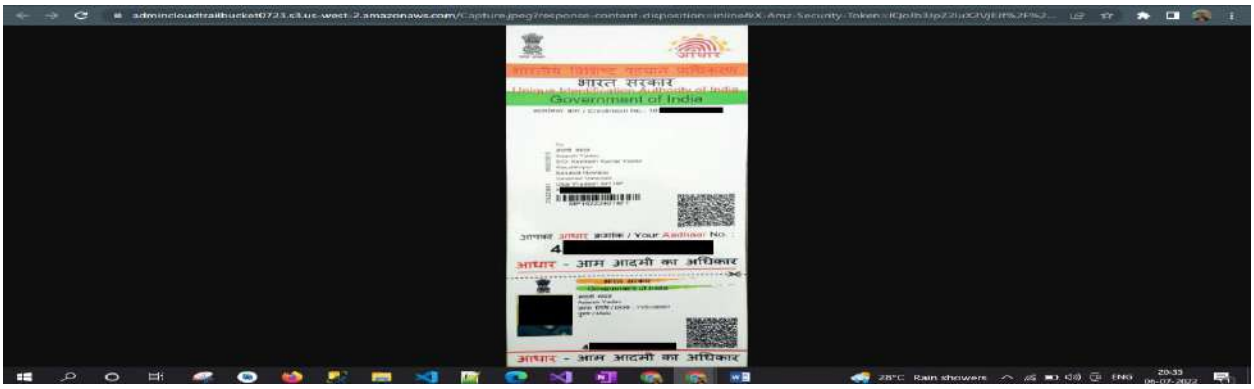
Task 4: Access the Encrypted Image

In this task, you will try to access the encrypted image through both the AWS management Console and the S3 link.

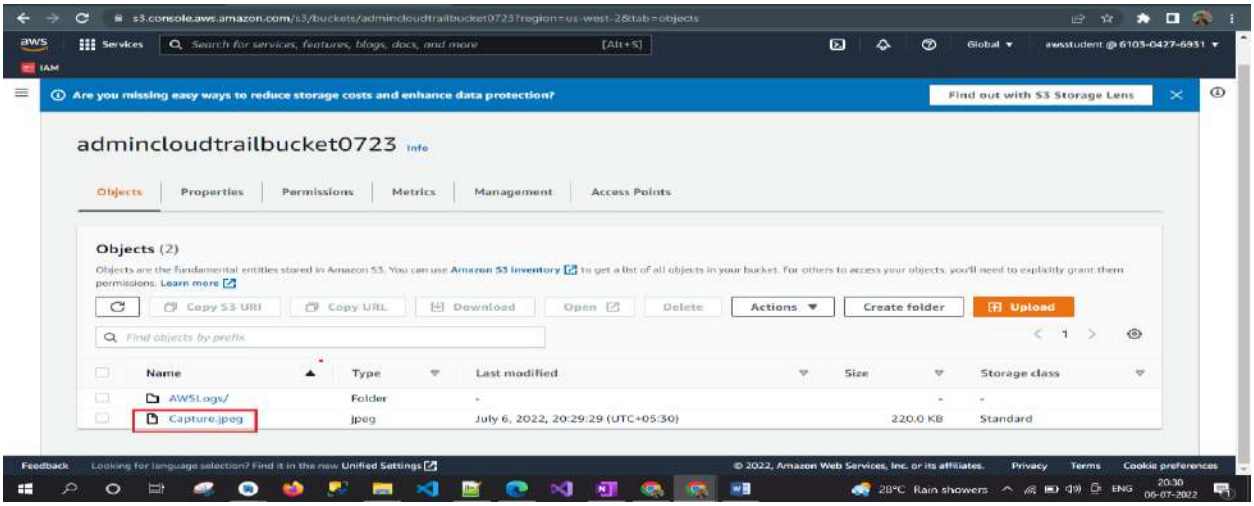
Step 39 – In the Object tab, select image name and then click Open.

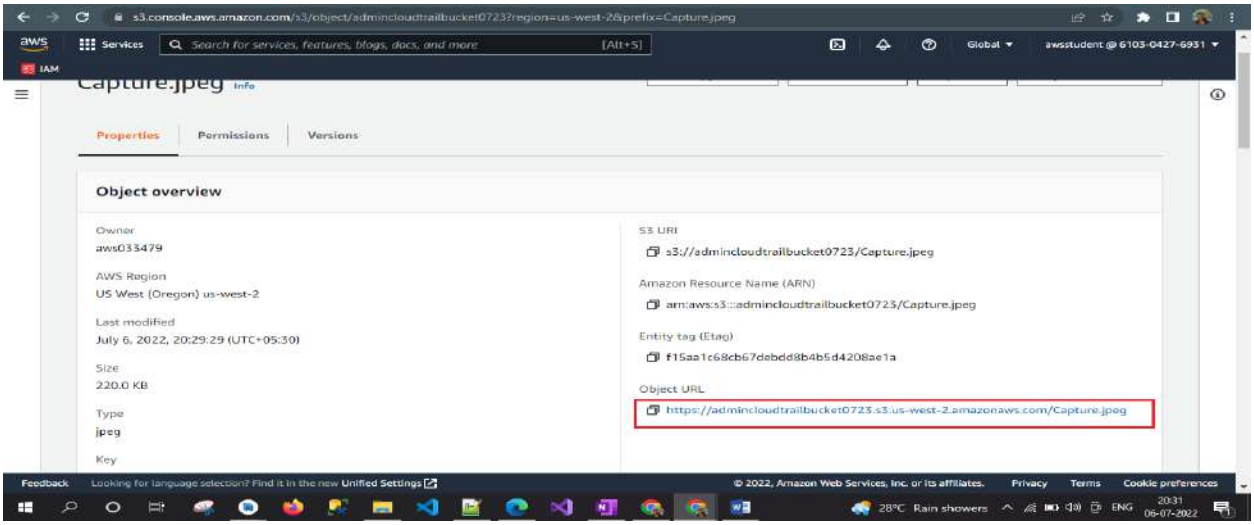


Step 40 – Choose the window/tab that shows your images.



Step 41 – Click the image name and copy the S3 object URL to your text editor.



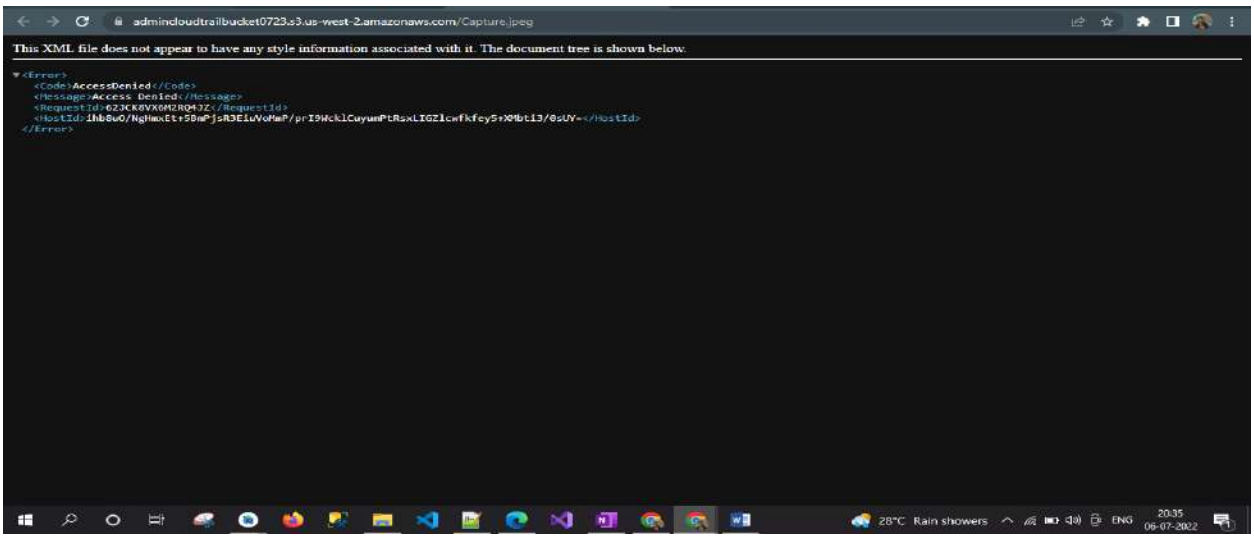


Step 42 – Paste the S3 object URL that you copied earlier into new browser/window.

Step 43 – Press **Enter**.

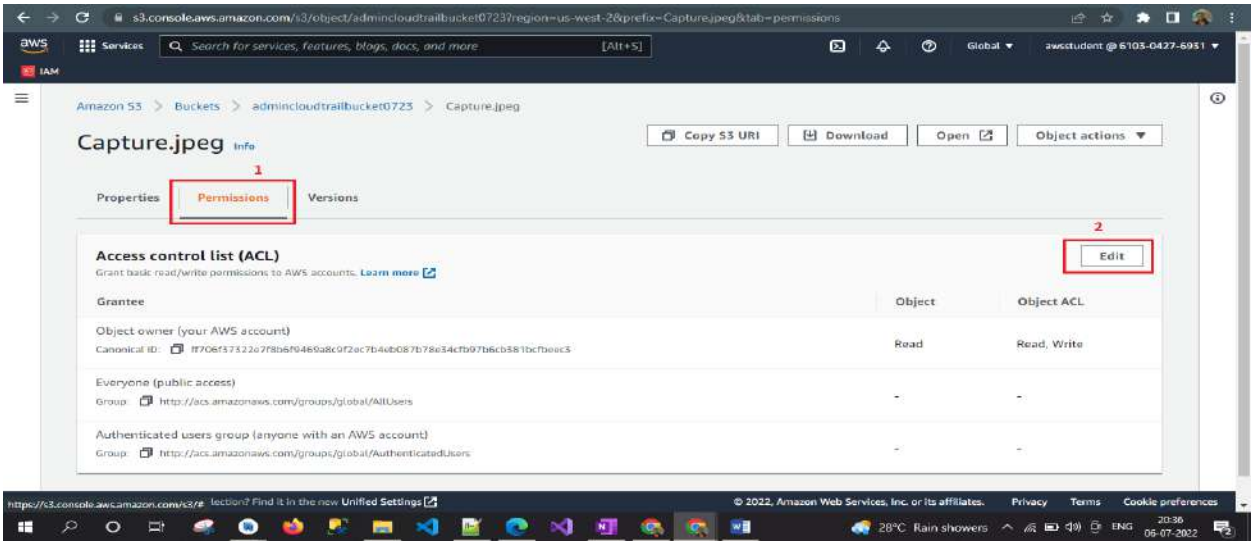
Step 44 – What does the page show?

It should show Access Denied. This is because, by default public access is not allowed.

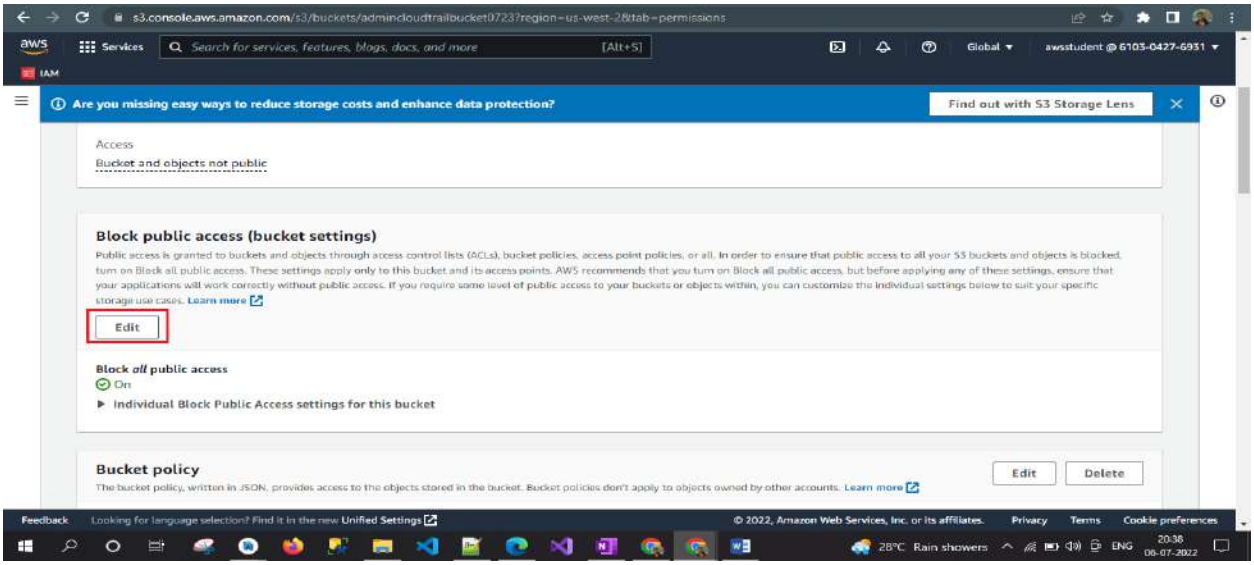


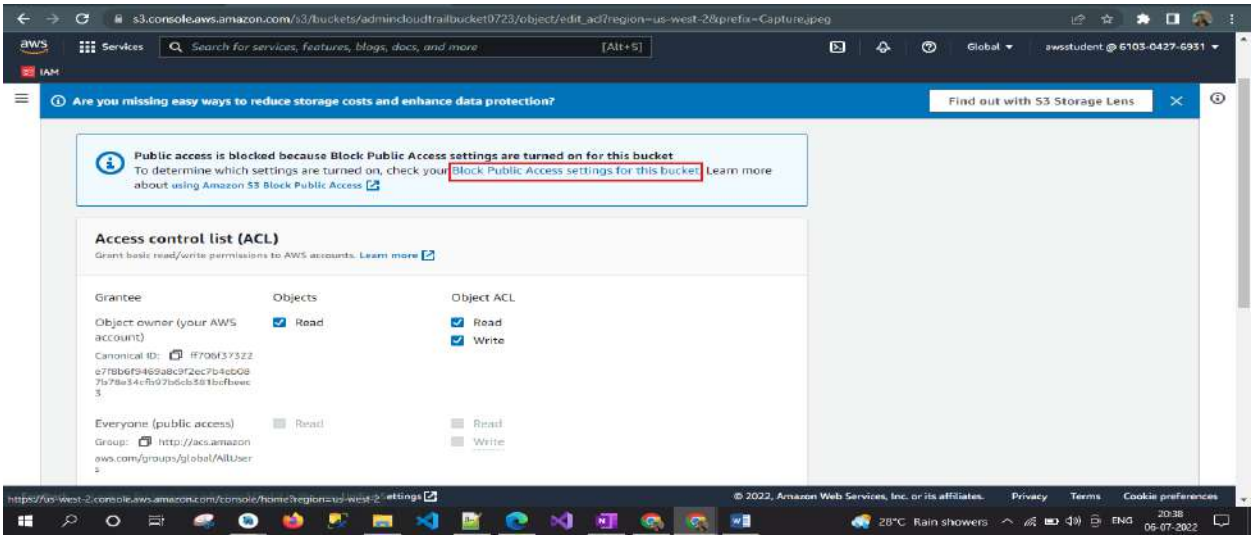
Step 45 – In the AWS Management Console, at the top of your screen, click the name of your bucket.

Step 46 – Click the Permission tab.

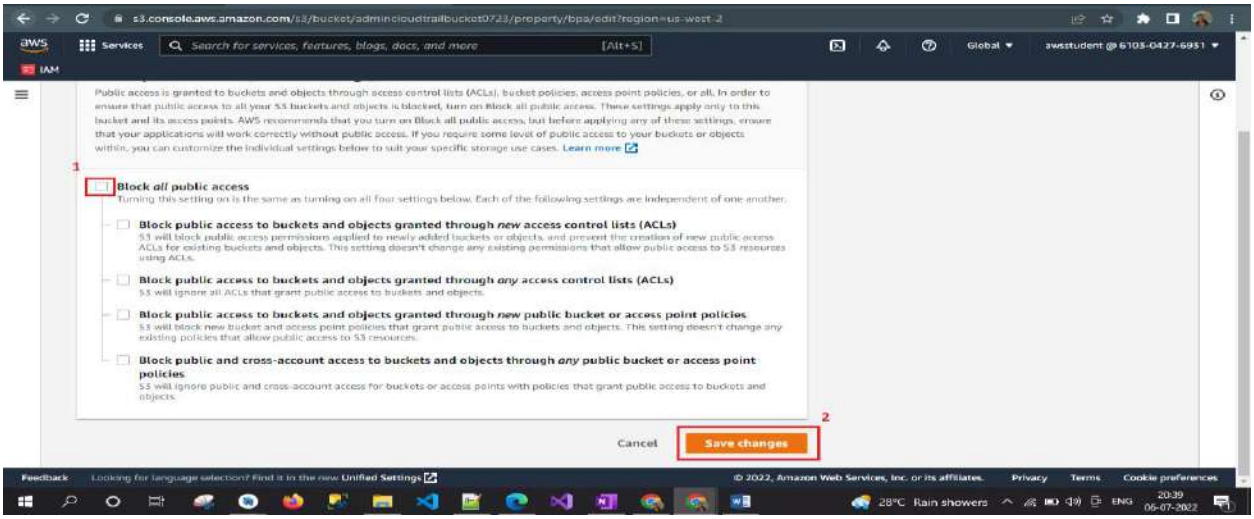


Step 47 – For Block public access (bucket settings), click Edit.



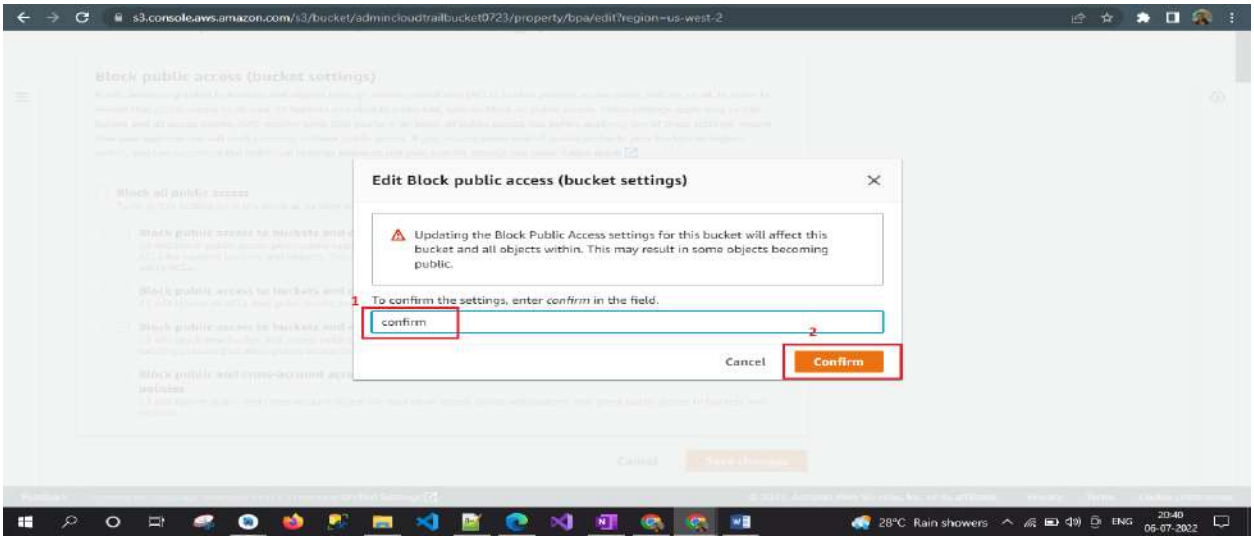


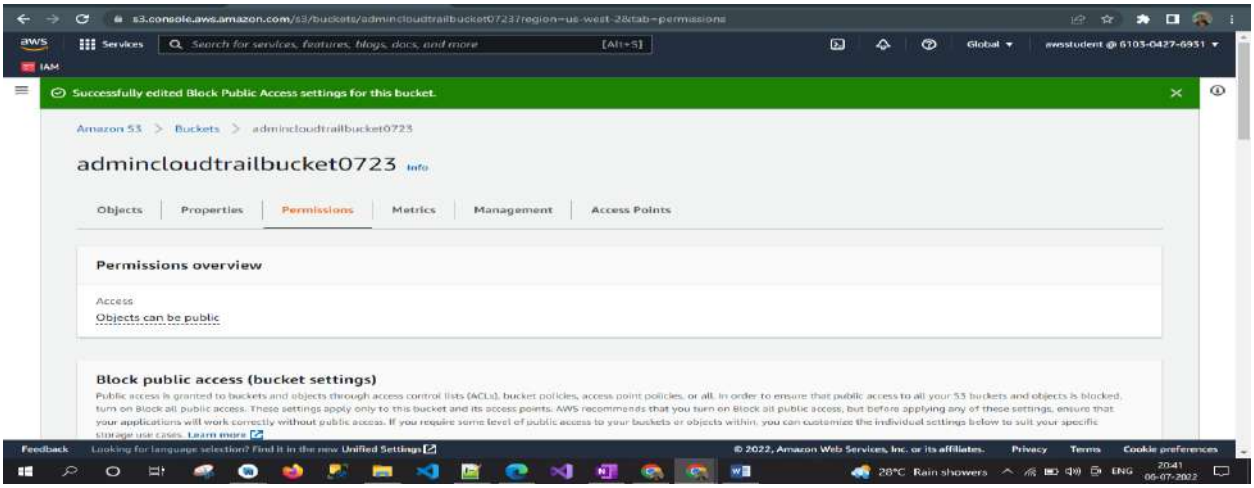
Step 48 – De-select Block all public access.



Step 49 – Click Save changes then:

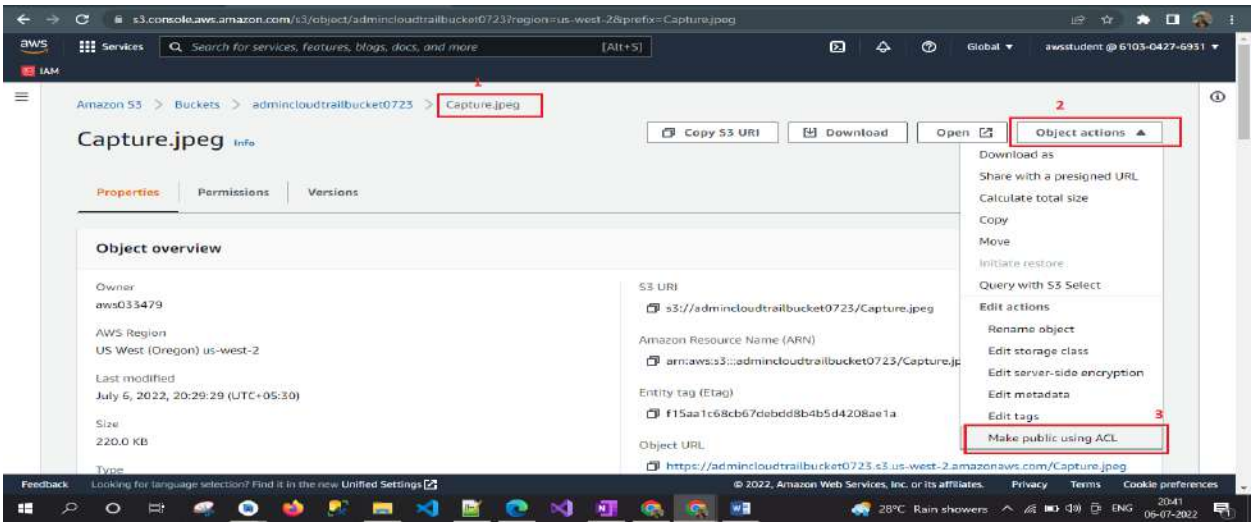
- **Type**: confirm
- **Click**: Confirm



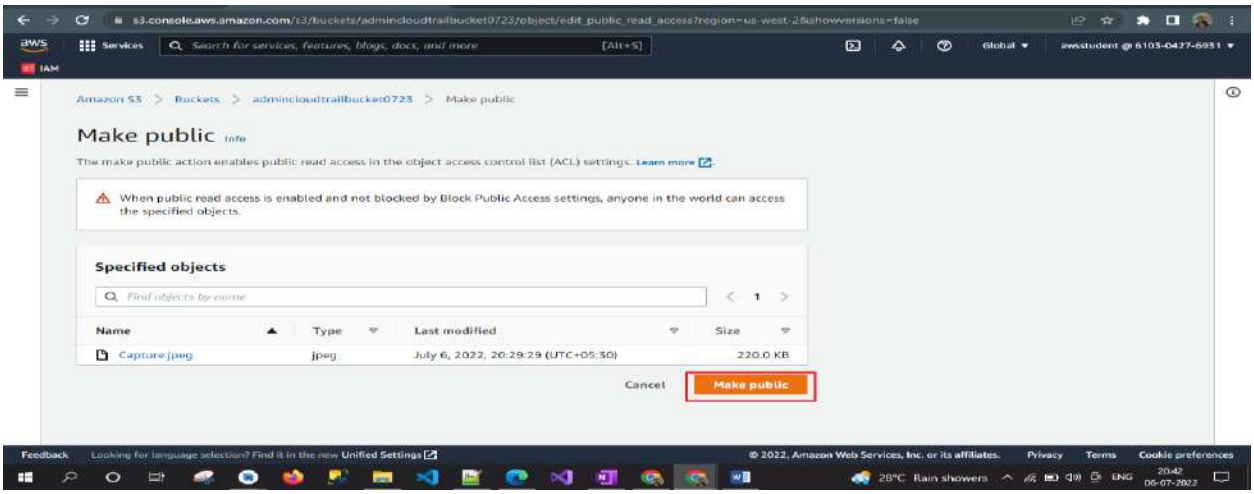


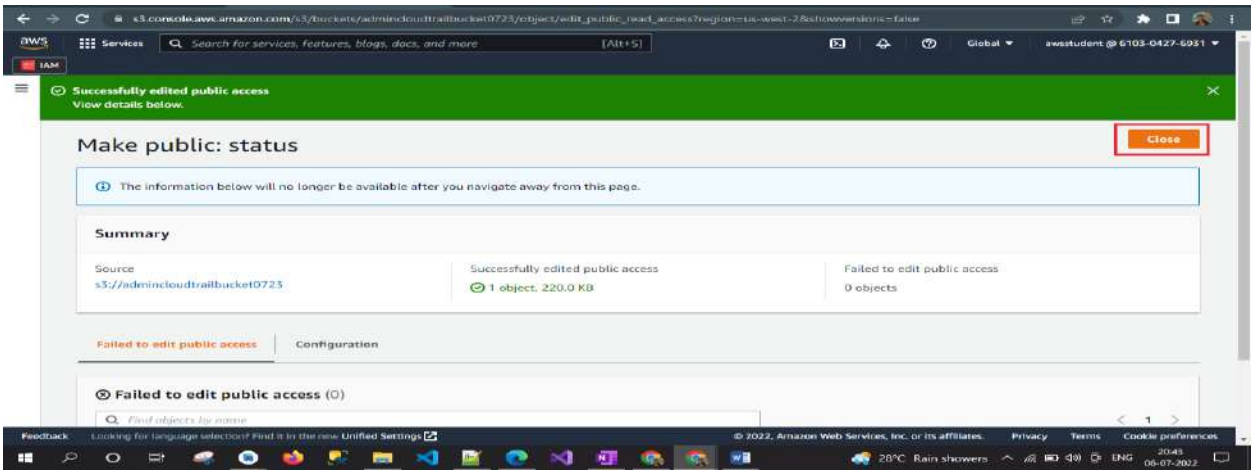
Step 50 – In the Object tab, select your image.

Step 51 – Click Action > **Make public using ACL**.

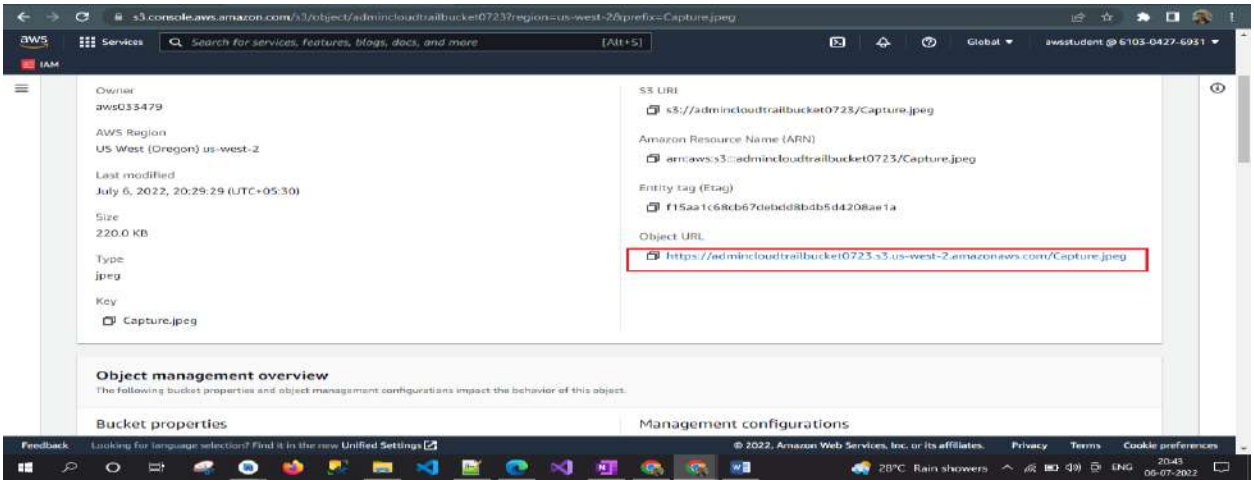


Step 52 – Click **Make public**.



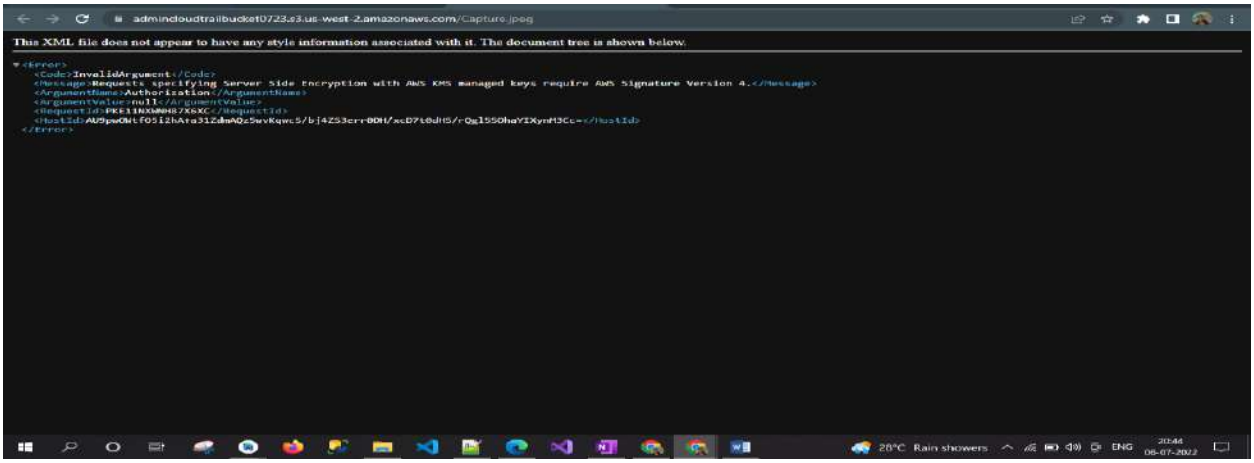


Step 53 – Refresh the screen for the new tab/window that you opened earlier.



Step 54 – What do you see?

Because the image is encrypted, you are not able to view it using public link. You should see the message saying request specifying server side encryption with AWS KMS managed key requires AWS signature version 4.



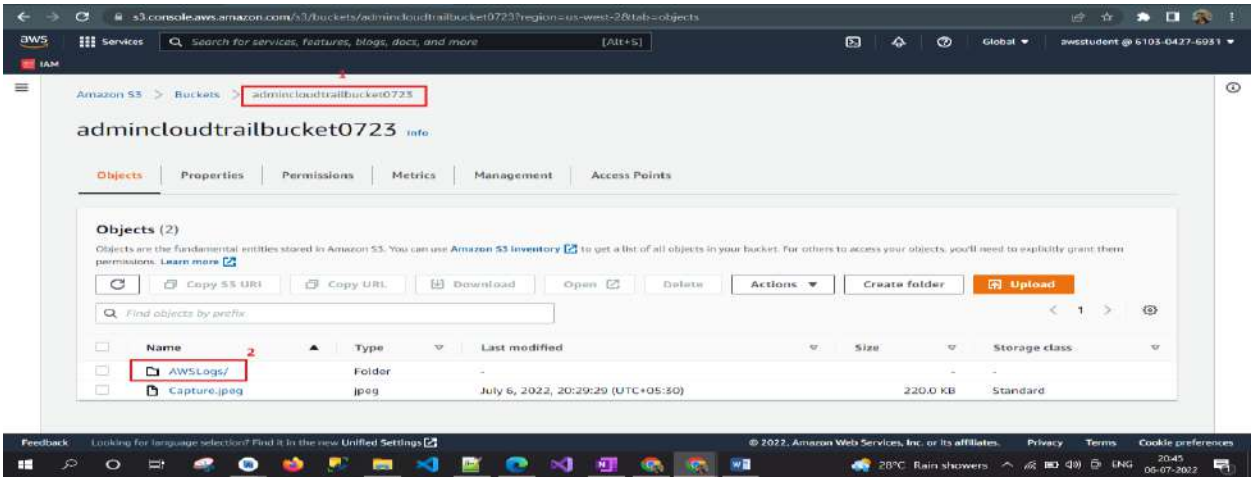
Step 55 – Close the new/tab window.

Task 5: Monitor KMS activity Using CloudTrail Logs.

In this task, you will access your CloudTrail log files and view logs related to your encryption operation.

Step 56 – In the AWS management console click Close.

Step 57 – Click the Object tab.



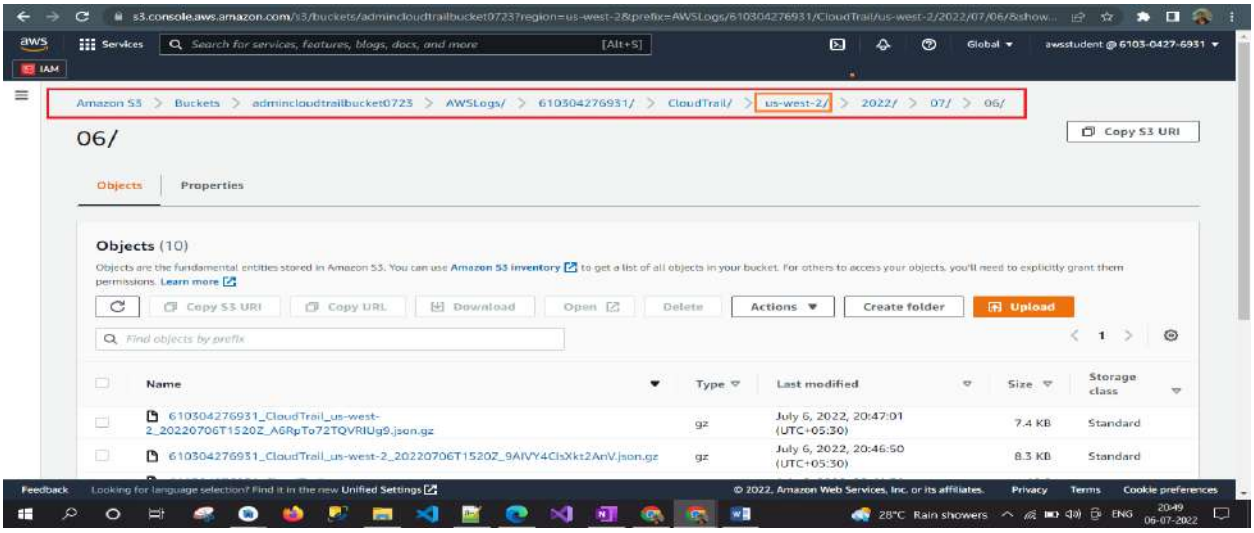
The path should look similar to:

Amazon S3 > AWSLogs > 197167081626 > CloudTrail > `Region` > 2019 > 07 > 10

In the above example, replace Region with the name of the region that you bucket was created in.

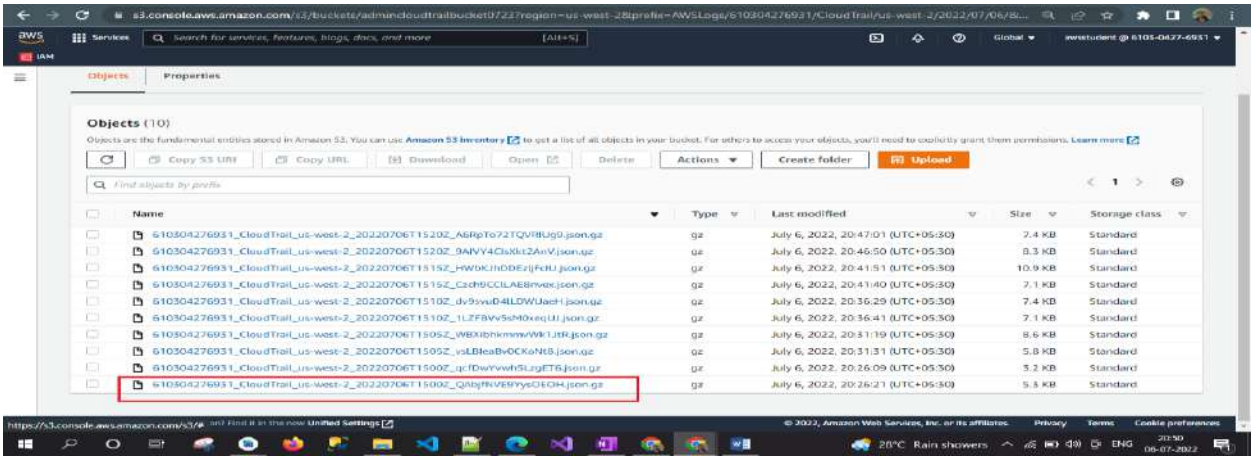
Note: If you don't see any log files, click the **refresh** button every few seconds till you see a log file.

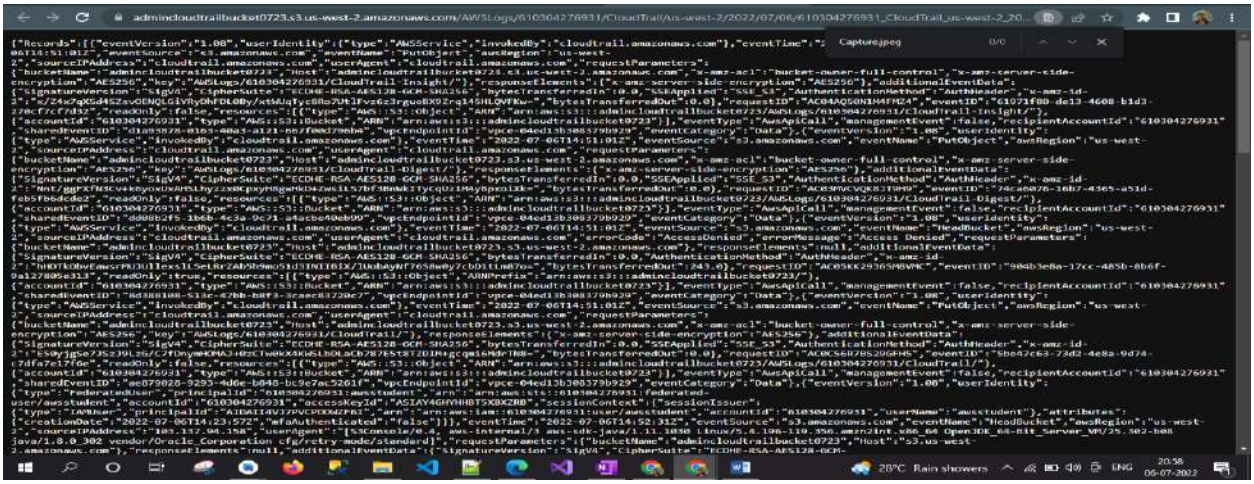
The log files will have an extension of ***.json.gz**



Step 58 – Drill down through the AWSLogs folders till you get to a folder that contains log file(s).

The path should similar to Amazon S3 > AWSLogs > 197167081626 > CloudTrail > 'Region' > 2019 > 07 >10





Step 59 – Do you see a log file whose Last modified date is later than the timestamp for the image file you downloaded?

Step 60 – if there is not a log file who's Last modified data is later than the timestamp for the uploaded image file, continue to click refresh button every few seconds till there is.

It can take up to 5 minutes to see a log file that has a Last modified time stamp that is greater than the time stamp of the image file that you uploaded.

Step 61 – Click the latest file in the list.

Step 62 – Click Open.

Step 63 – If you see a pop-up security warning, confirm that you want to open the file. If not, continue to the next step.

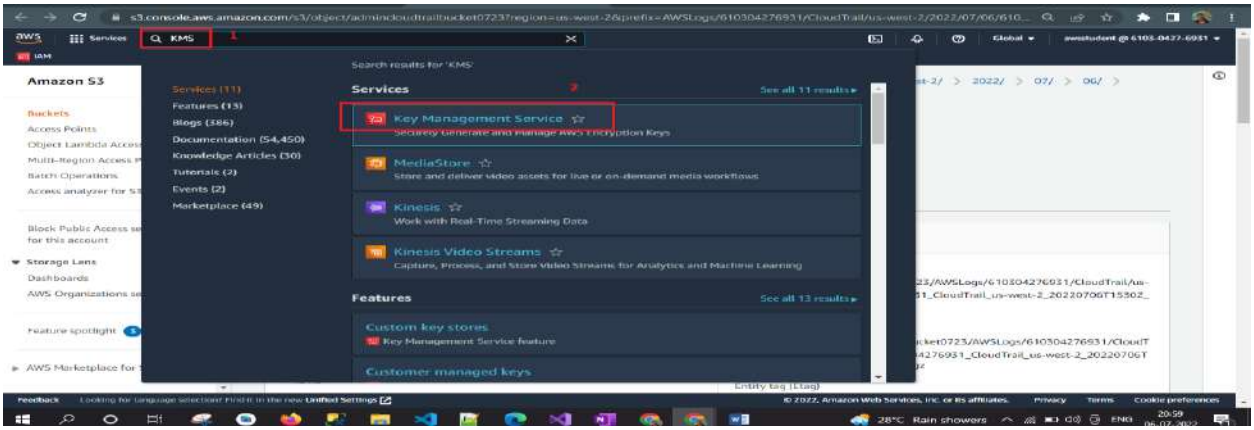
Step 64 – Search for the following in your log file:

- Your encryption Key ID that you copied to your text editor.
- The name of the file that you upload (you should see the name of the file in the same log file that contains your encryption key id).

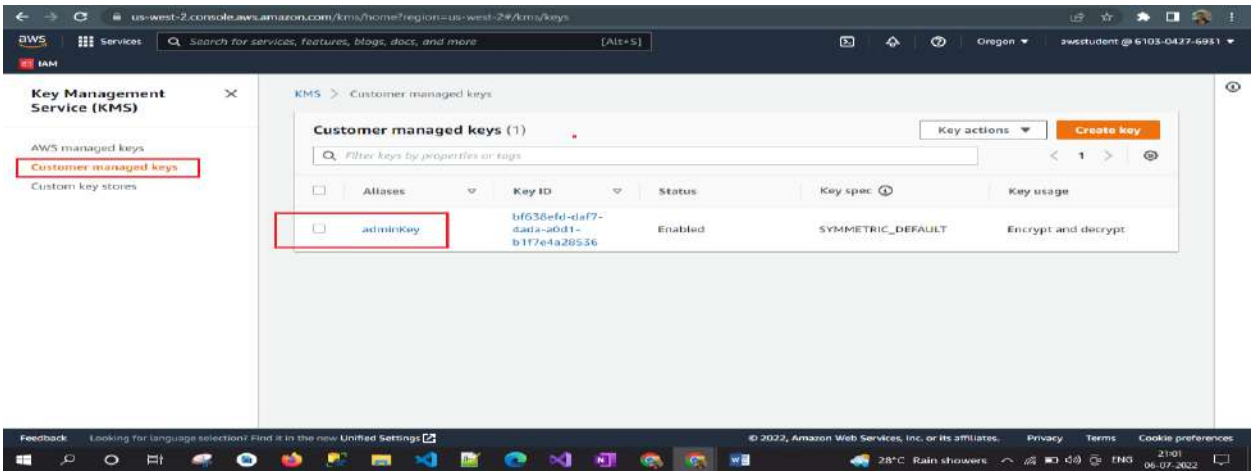
Task 6: Manage Encryption Keys.

In this task you will manage encryption key for users and role.

Step 65 – On the **Service** menu, click **Key Management Services**.



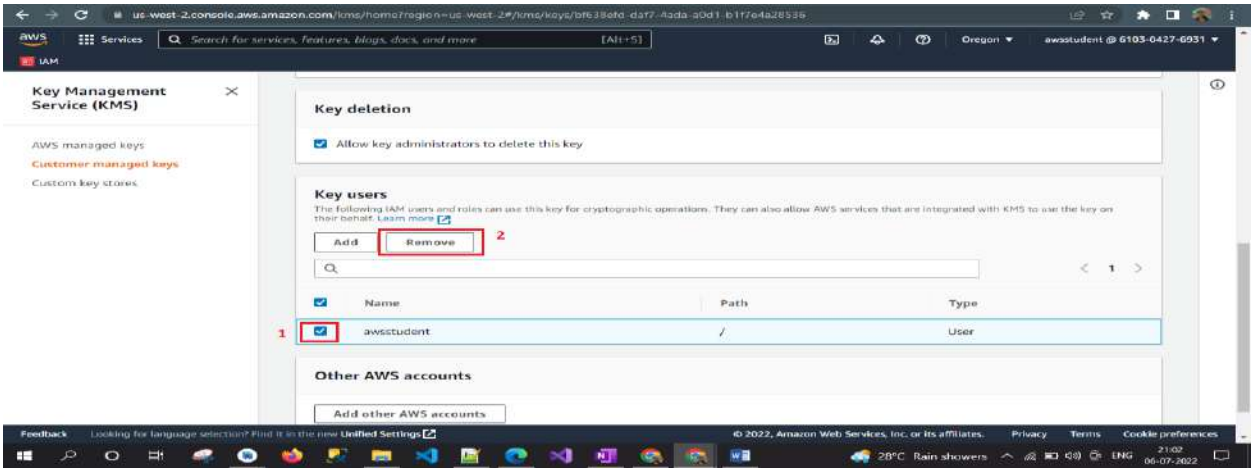
Step 66 – Click adminKey.



Step 67 – In the Key users Section, select the user or role that you signed with.

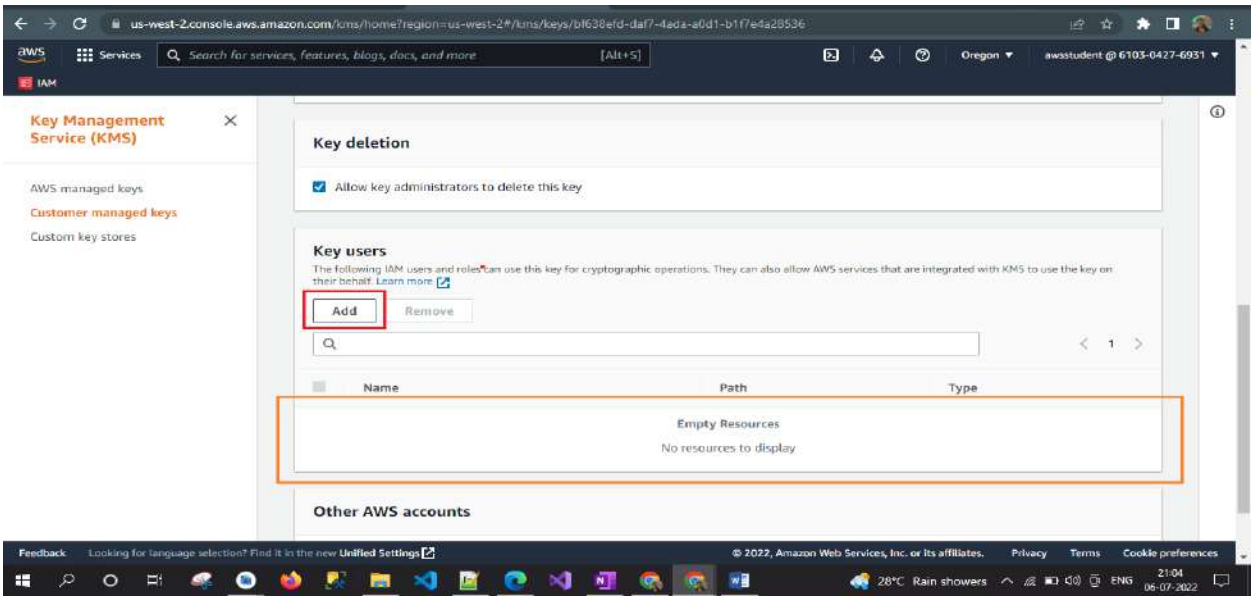
Step 68 – Click the Remove.

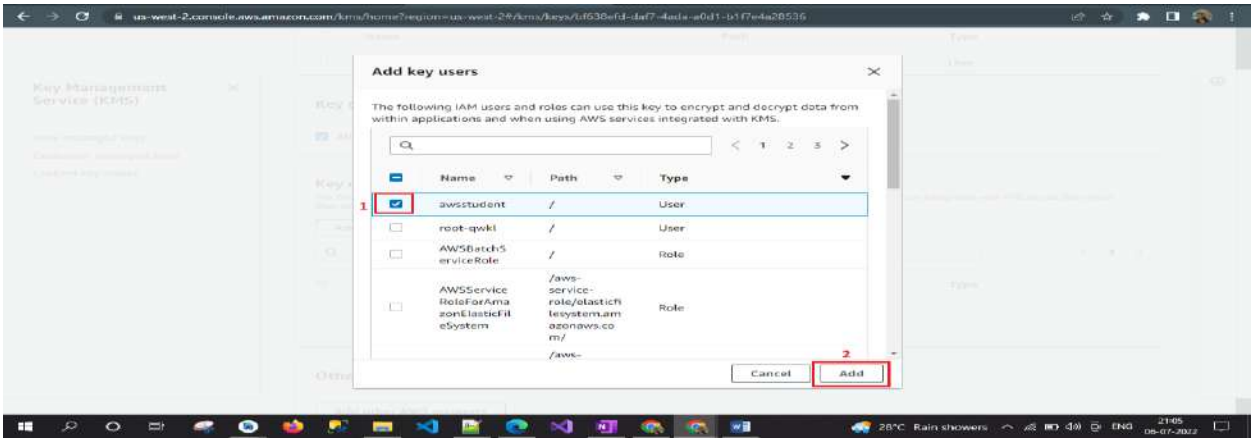
You have to remove the user's permissions to use this Key.



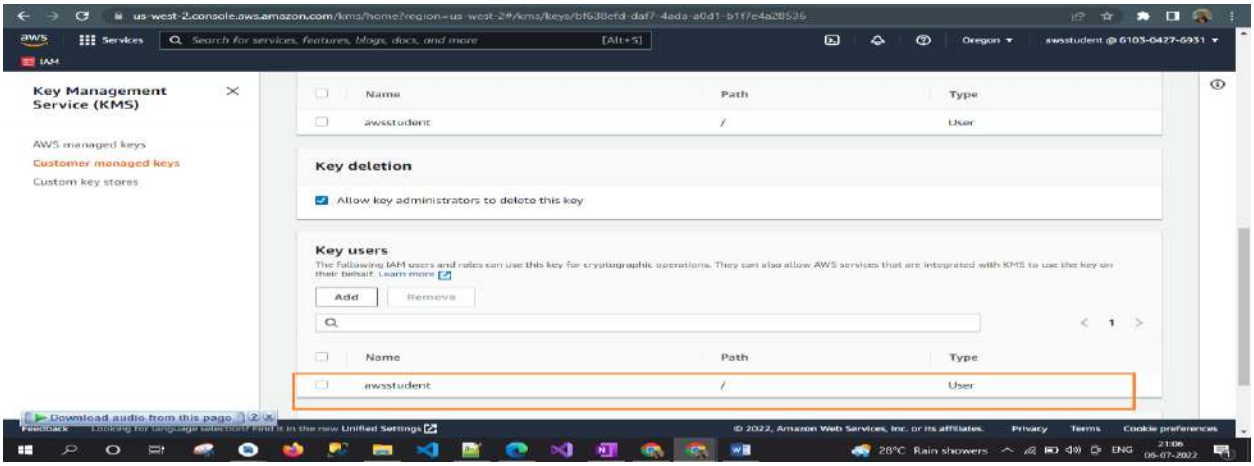
Step 69 – In the Key user section, Click the Add then:

- Select the user or role that you are signed with
- Click Add.

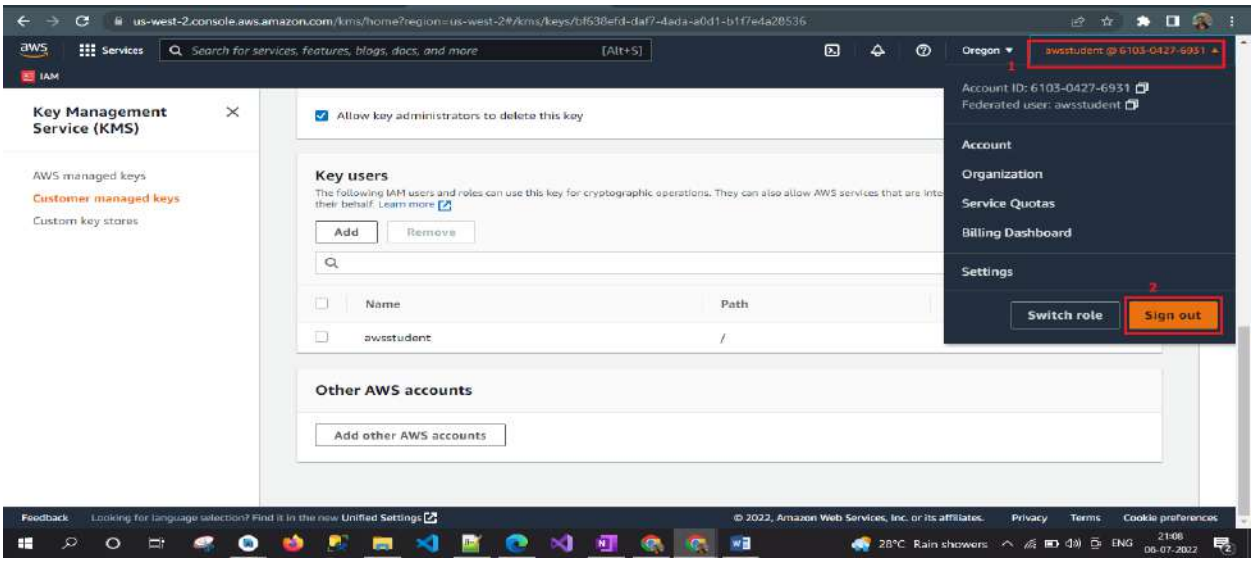




This shows how you can control which IAM users or role can use KMS keys the you create. The Same add and remove steps are used to control which IAM users can manage KMS Keys.



On the navigation bar, choose **awsstudent@<AccountNumber>**, and then click on the **Sign Out** button



After the sigout then click on the **End Lab**

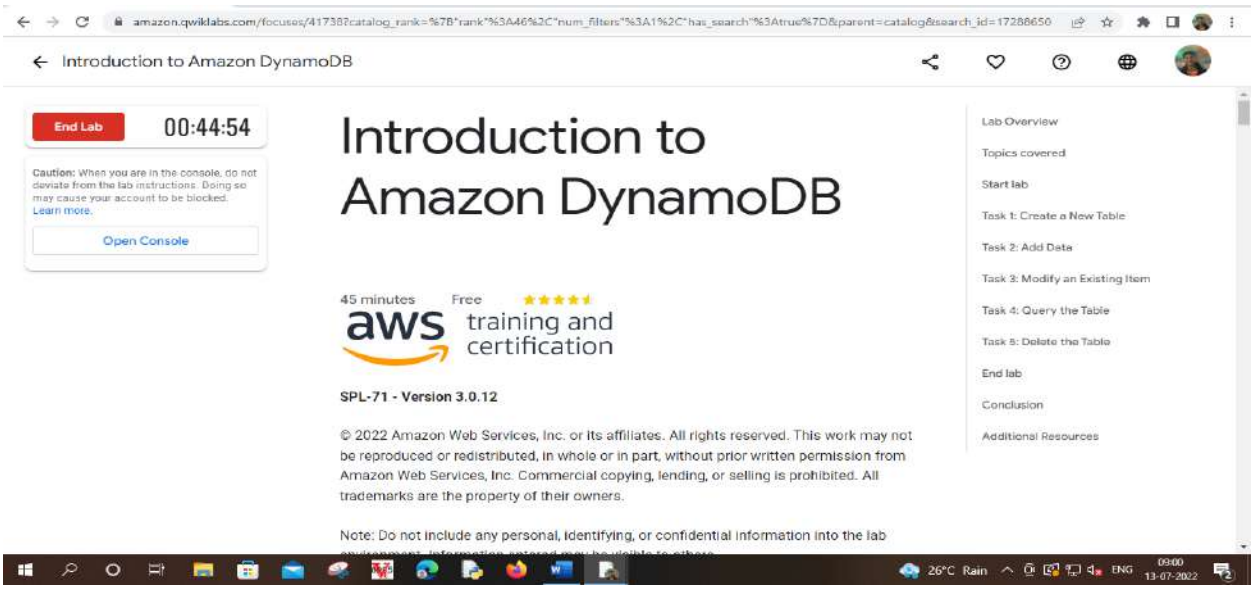
Practical 5: Introduction to Amazon DynamoDB

A. Create a new table
B. Add data
C. Modify existing items
D. Query the table
E. Delete the table

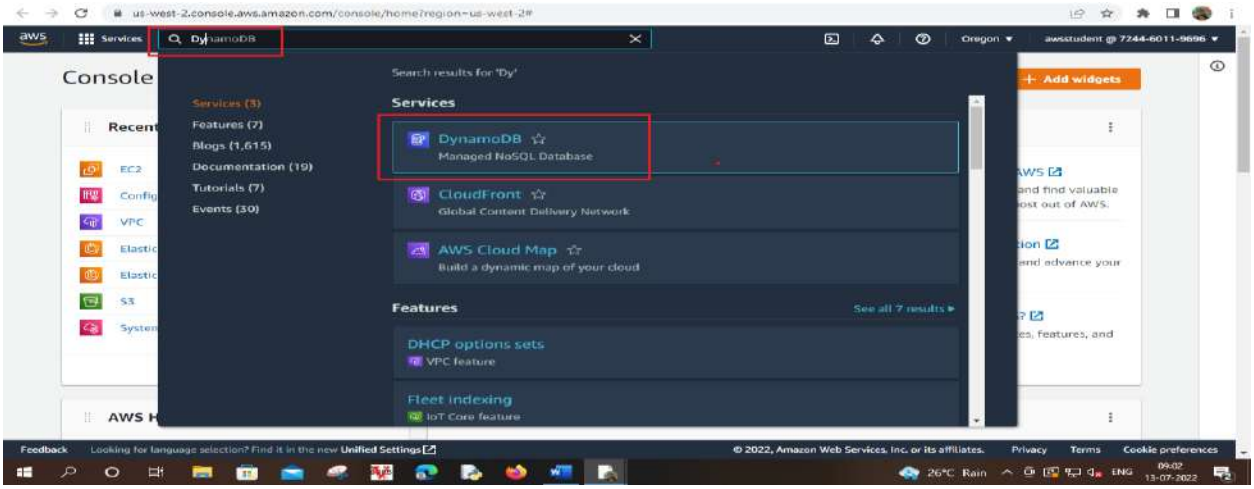
Task 1: Create an Amazon DynamoDB table

Go to the given link
https://amazon.qwiklabs.com/focuses/41738?catalog_rank=%7B%22rank%22%3A46%2C%22num_filters%22%3A1%2C%22has_search%22%3Atrue%7D&parent=catalog&search_id=17288650

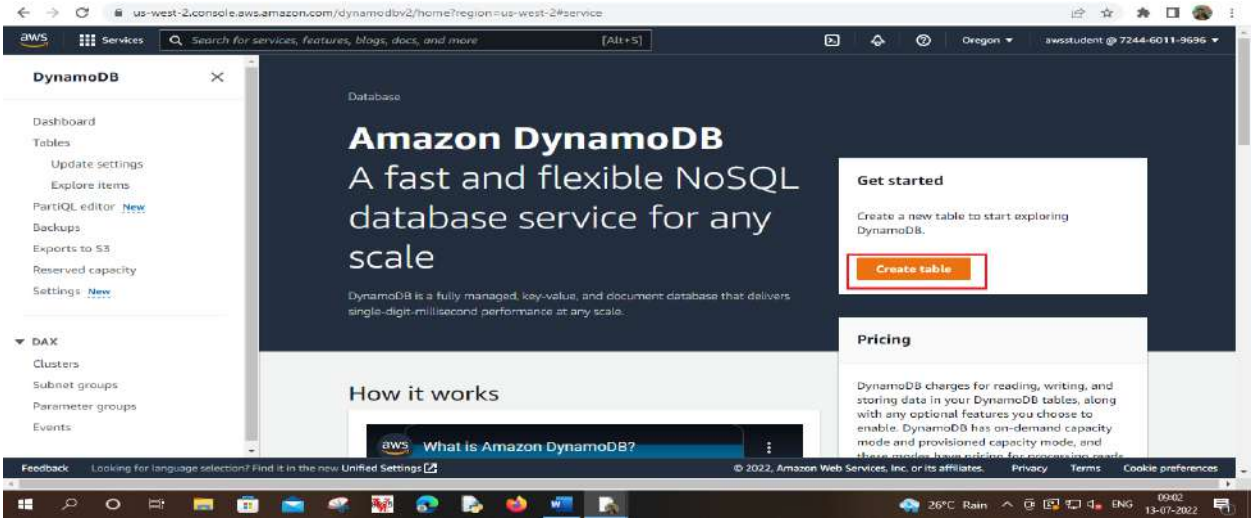
Step 1 – To launch the lab, at the top of the page, choose **Start Lab** button & To open the lab, choose **Open Console** button



Step 2 – In the AWS Management Console, choose **Services**, and then choose **DynamoDB**



Step 3 – Choose Create table.

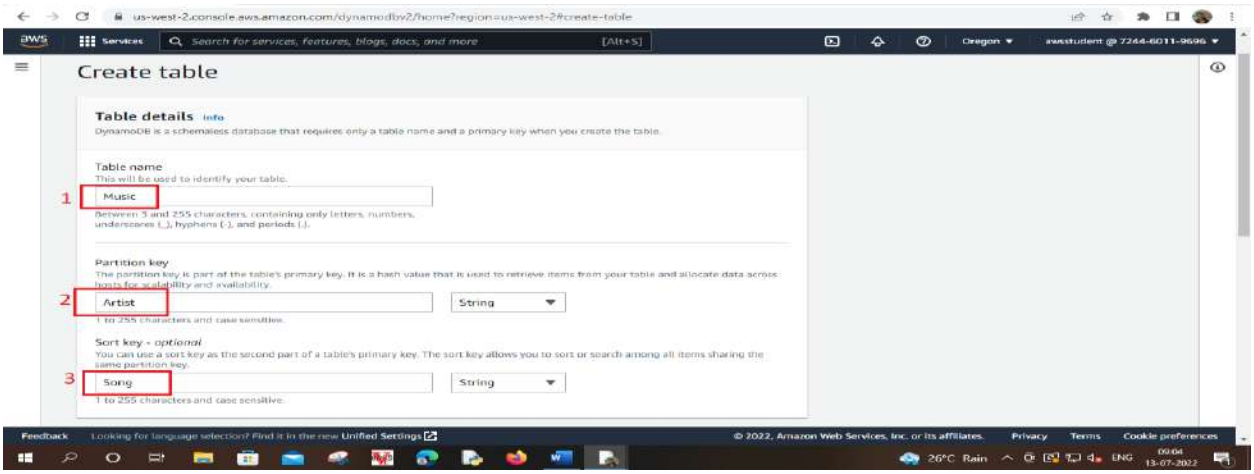


Step 4 – For **Table name**, type: Music

Step 5 – For **Partition key**, type Artist and leave **String** selected.

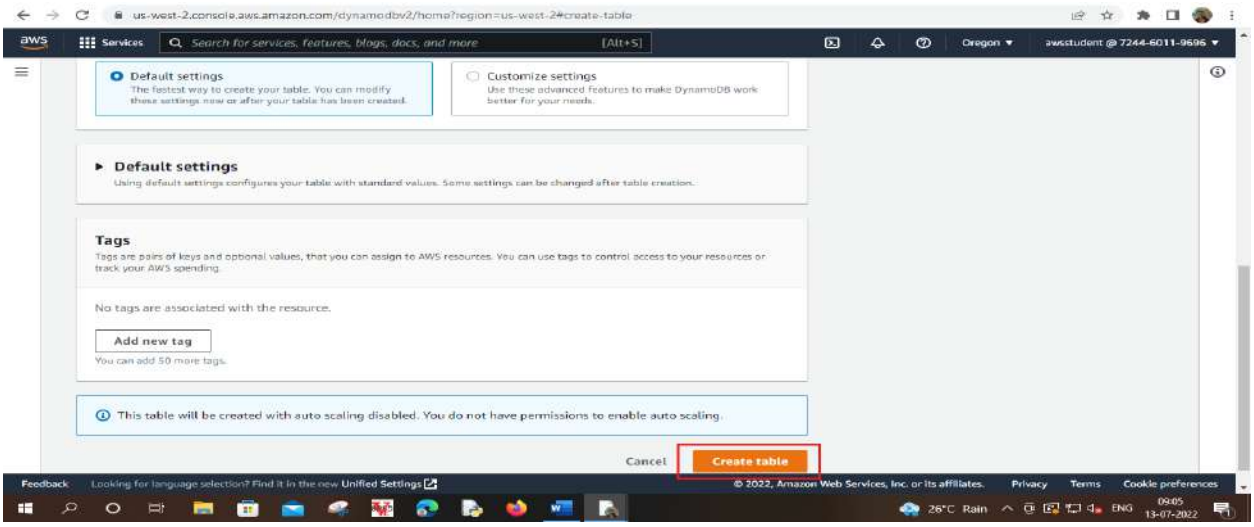
Step 6 – For **Sort Key**, type Song.

Your table will use default settings for indexes and provisioned capacity.

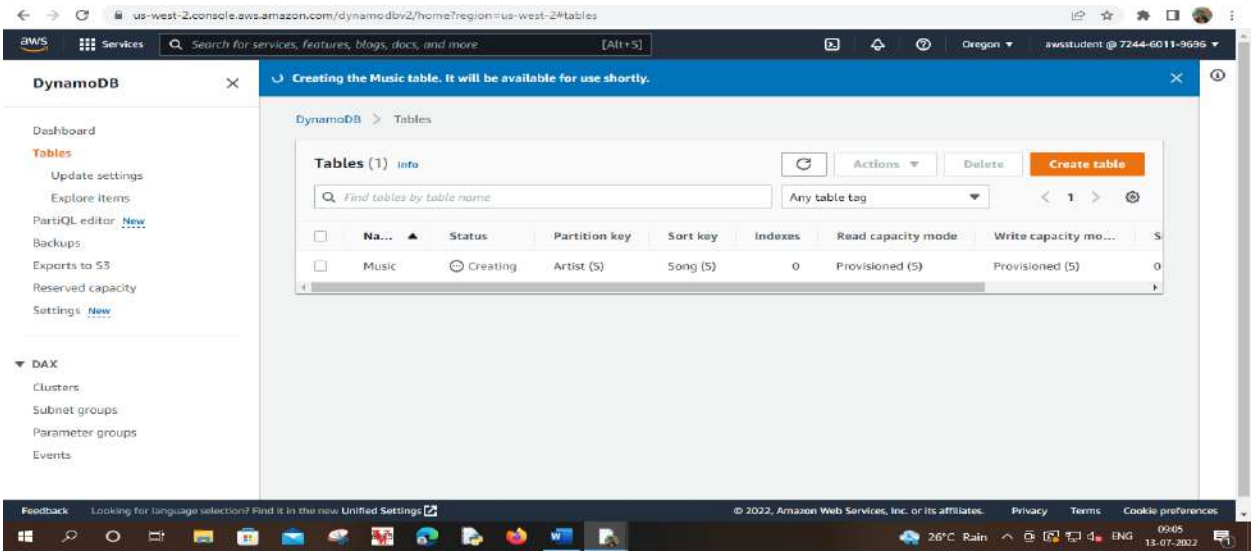


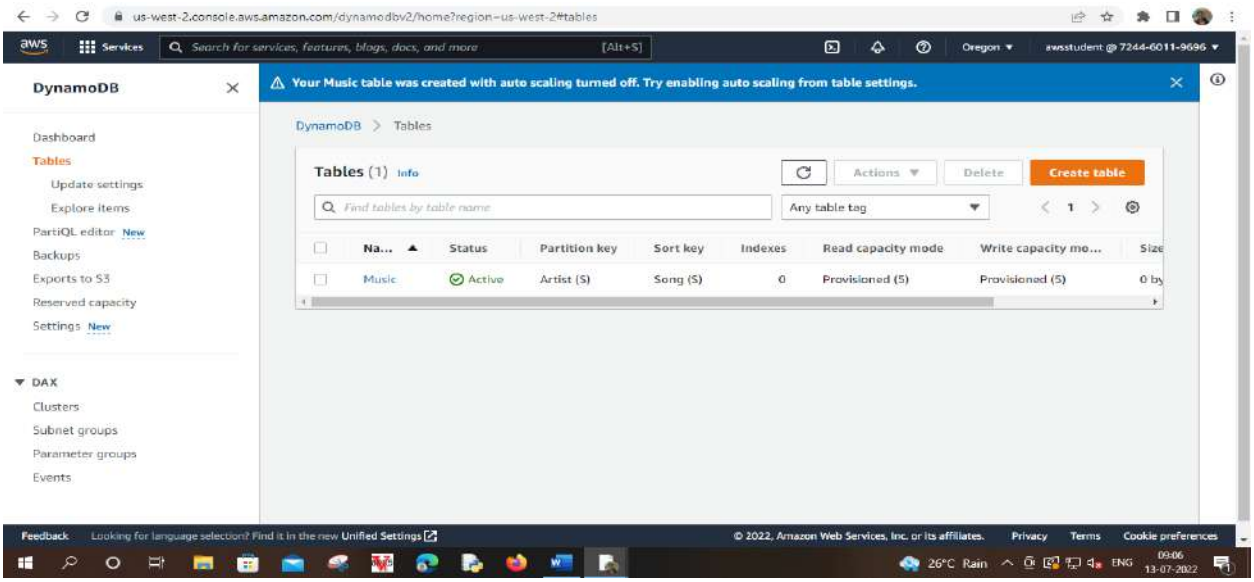
Step 7 – Choose **Create table**.

The table will be created in less than a minute.



Step 8 – Wait for your table to be created.





Task 2: Add Data

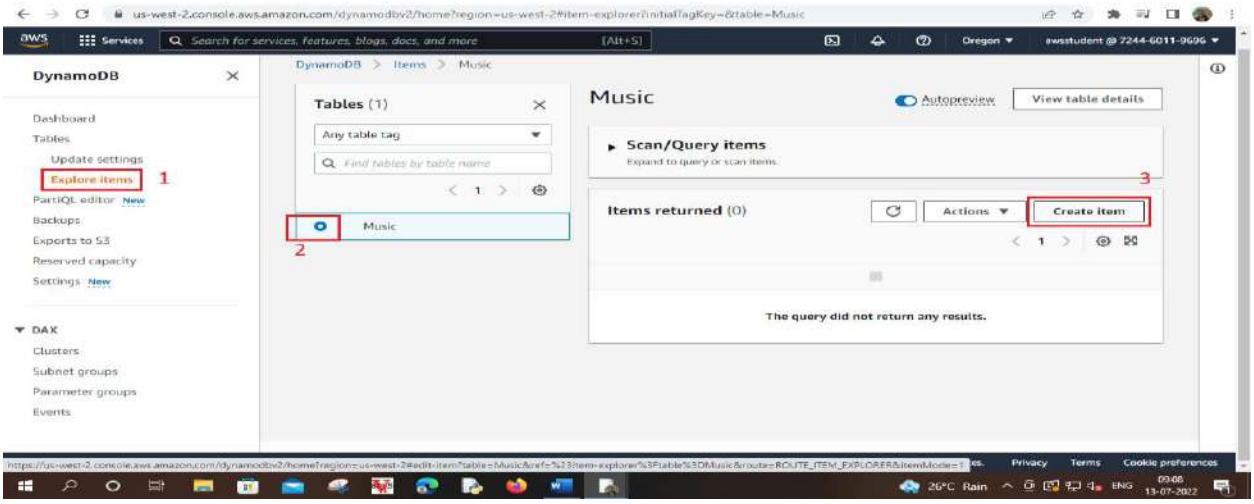
In this task, you will add data to the table. A table is a collection of data on a particular topic.

Each table contains multiple **items**. An item is a group of attributes that is uniquely identifiable among all of the other items. Items in DynamoDB are similar in many ways to rows in other database systems. In DynamoDB, there is no limit to the number of items you can store in a table.

Each item is composed of one or more **attributes**. An attribute is a fundamental data element, something that does not need to be broken down any further. For example, an item in a Music table contains attributes such as Song and Artist. Attributes in DynamoDB are similar columns in other database systems, but each item (row) can have different attributes (columns).

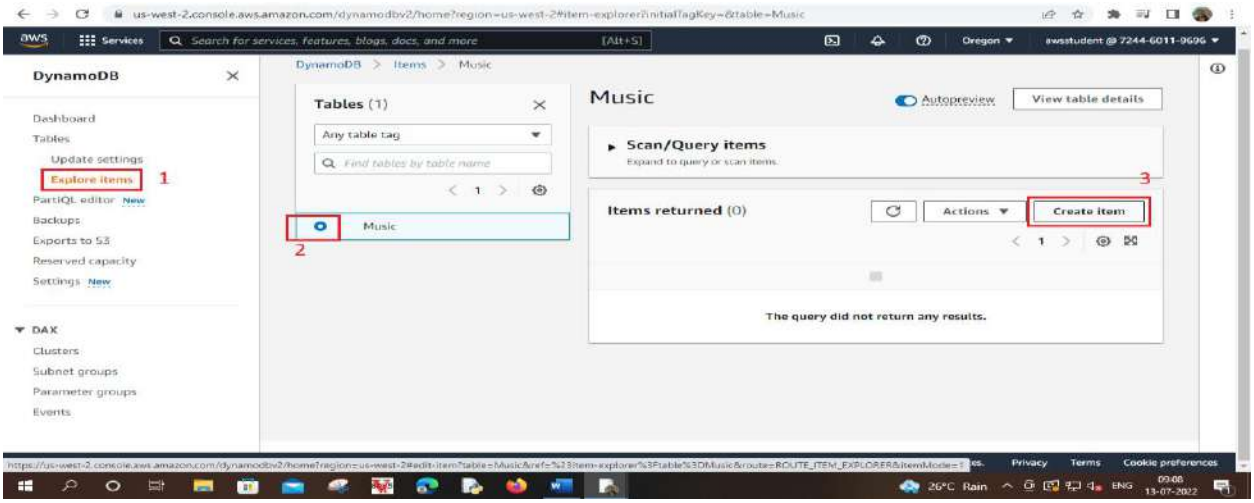
When you write an item to a DynamoDB table, only the Primary Key and Sort Key (if used) are required. Other than these fields, the table does not require a schema. This means that you can add attributes to one item that may be different to the attributes on other items.

Step 9 – In the left navigation pane, choose **Explore items.**



Step 10 – Select **Music**.

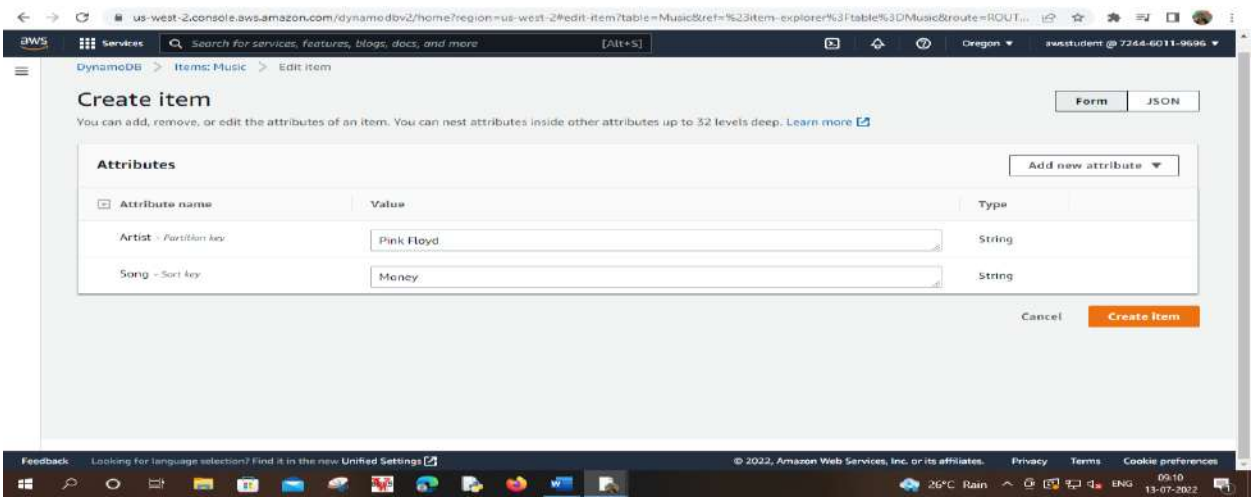
Step 11 – Choose **Create Item**.



Step 12 – For **Artist** String, type: **Pink Floyd**

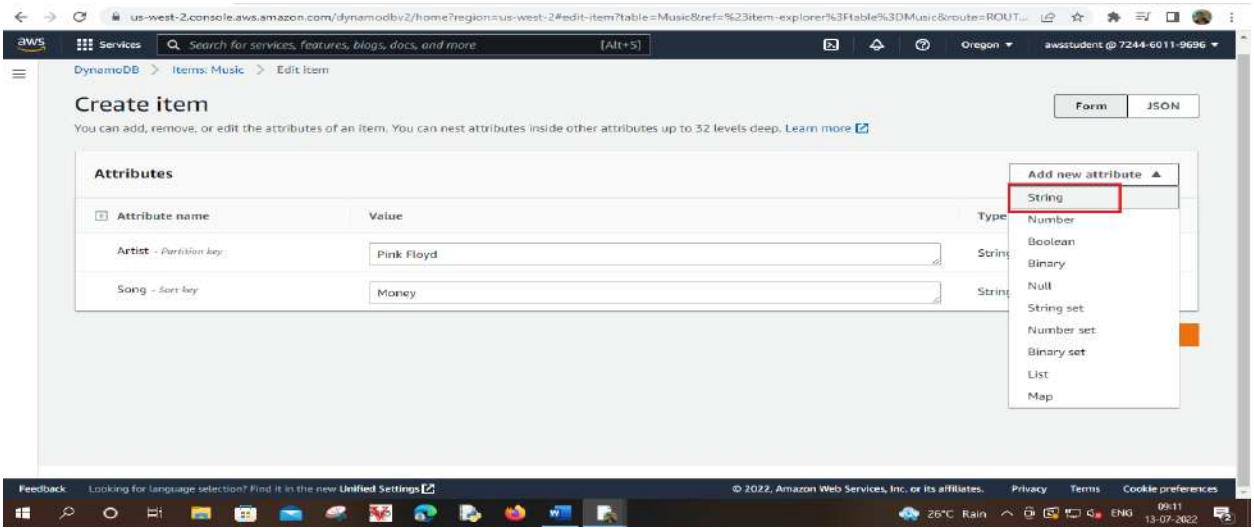
Step 13 – For **Song** String, type: **Money**.

These are the only required attributes, but you will now add additional attributes.



Step 14 – Click Create trail then configure to create an additional attribute, choose **Add new attribute.**

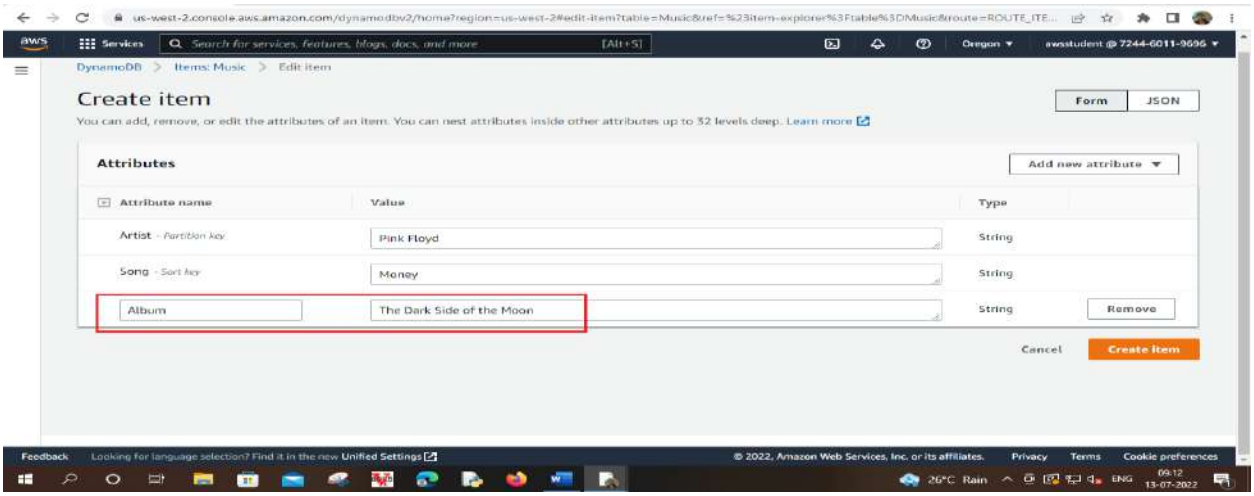
Step 15 – In the drop-down list, select **String**.



A new attribute row will be added.

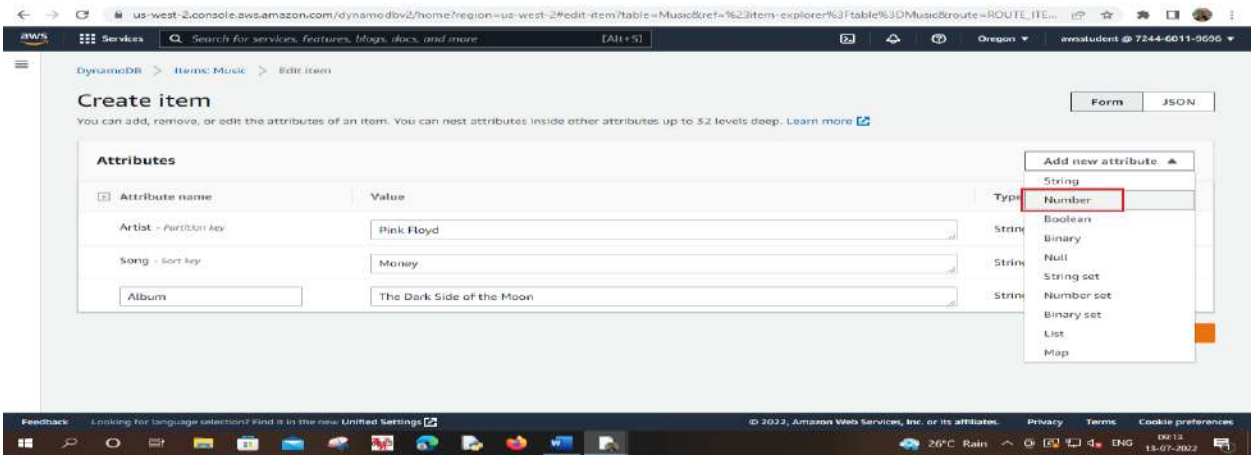
Step 16 – For the new attribute, enter:

- In **FIELD**, type: Album
- In **VALUE**, type: The Dark Side of the Moon



Step 17 – Add another new attribute.

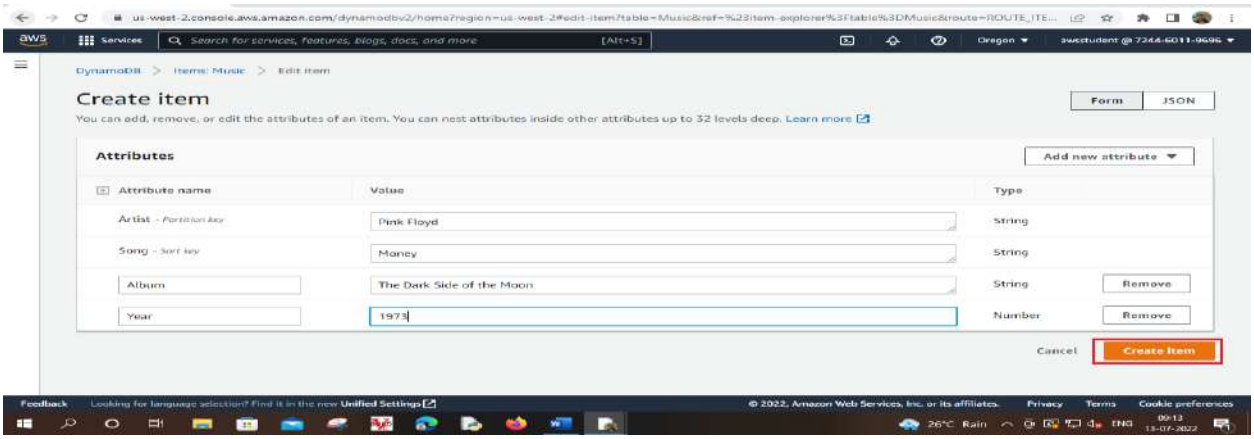
In the drop-down list select **Number**.



A new number attribute will be added.

Step 18 – For the new attribute, enter:

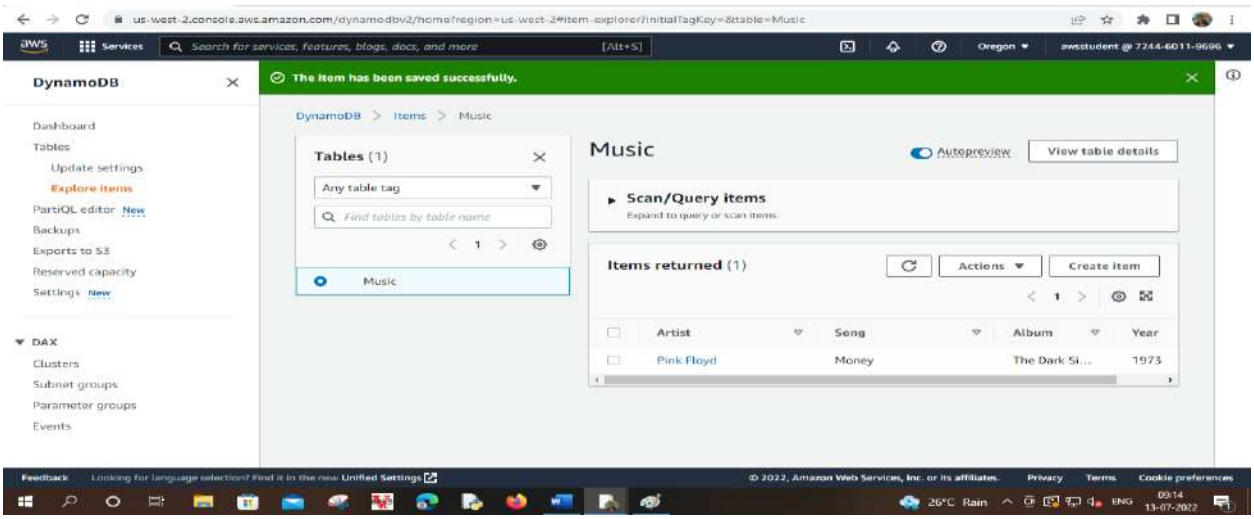
- In **FIELD**, type: Year
- In **VALUE**, type: 1973



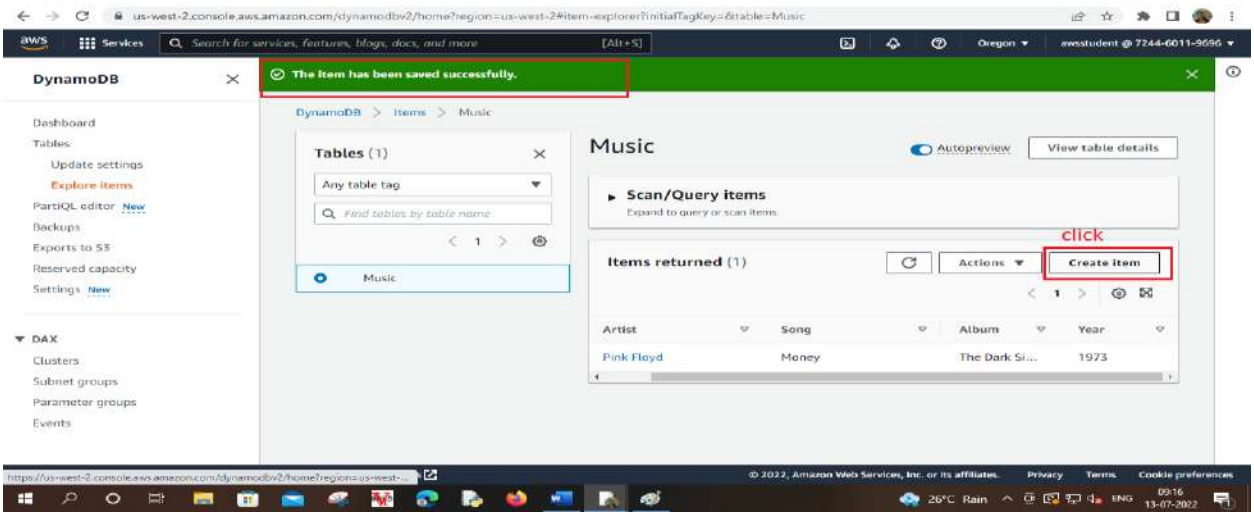
Step 19 – Choose Save changes.

Step 20 – Choose Create item to store the new Item with its four attributes.

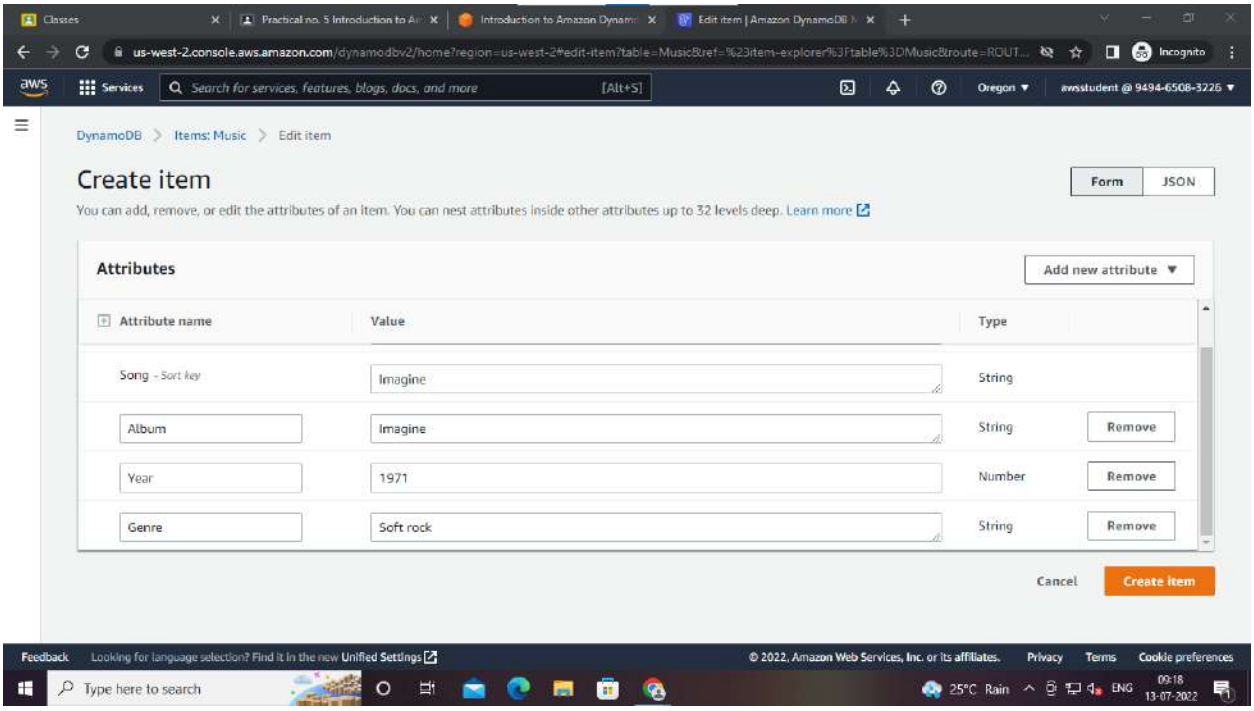
The item will appear in the console.



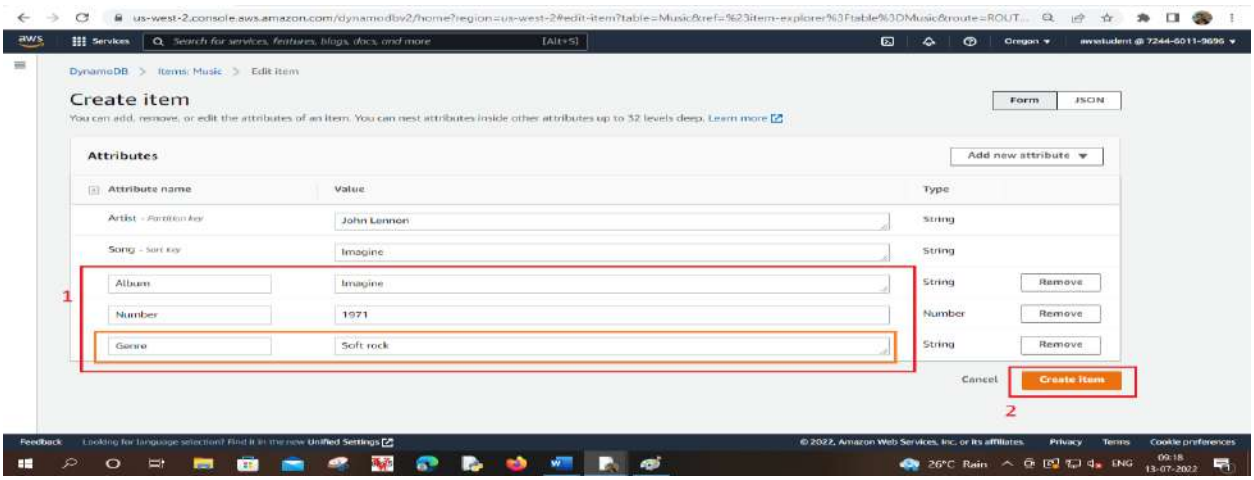
Step 21 – Now create a second Item, using these attributes:

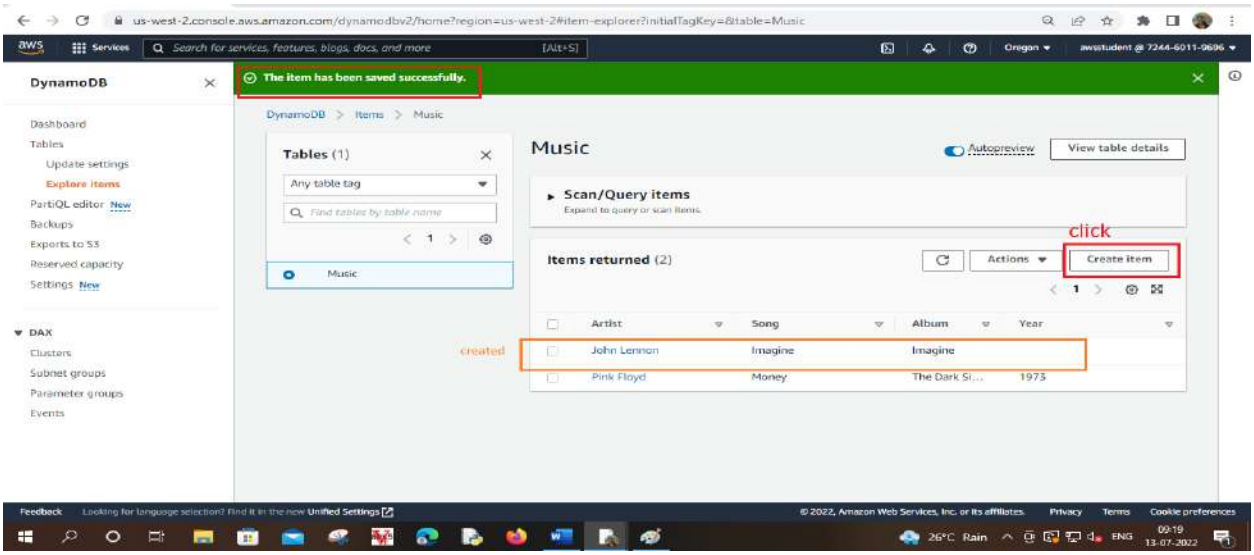


Attribute Name	Attribute Type	Attribute Value
Artist	String	John Lennon
Song	String	Imagine
Album	String	Imagine
Year	Number	1971
Genre	String	Soft rock



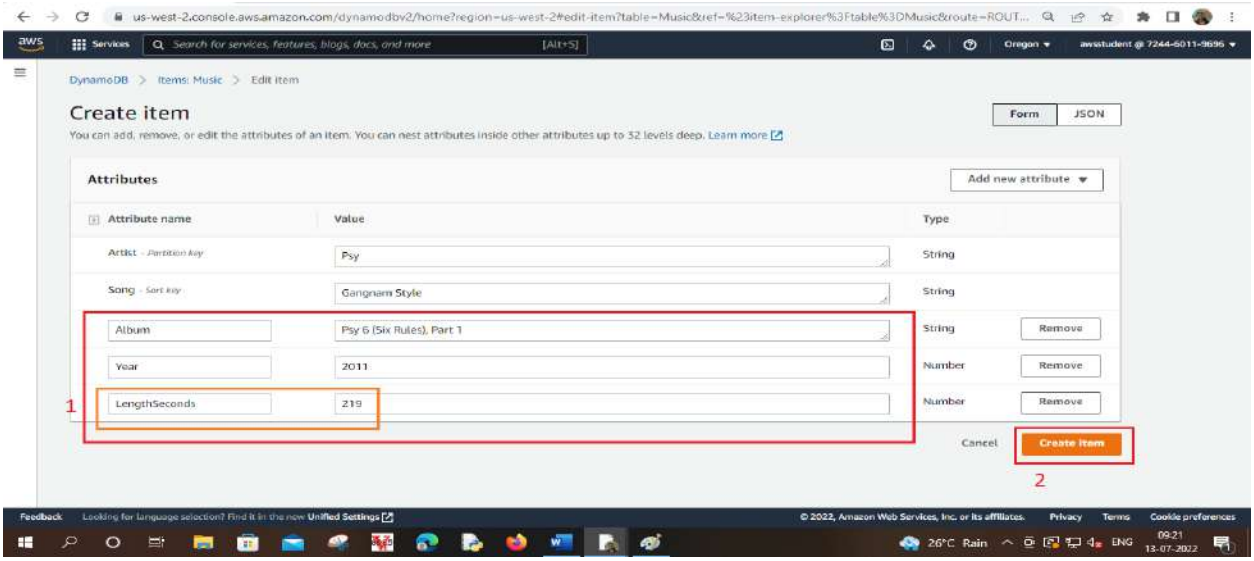
Note: This item has an additional attribute called genre. This is an example of each item being capable of having different attributes without having to pre-define a table schema.

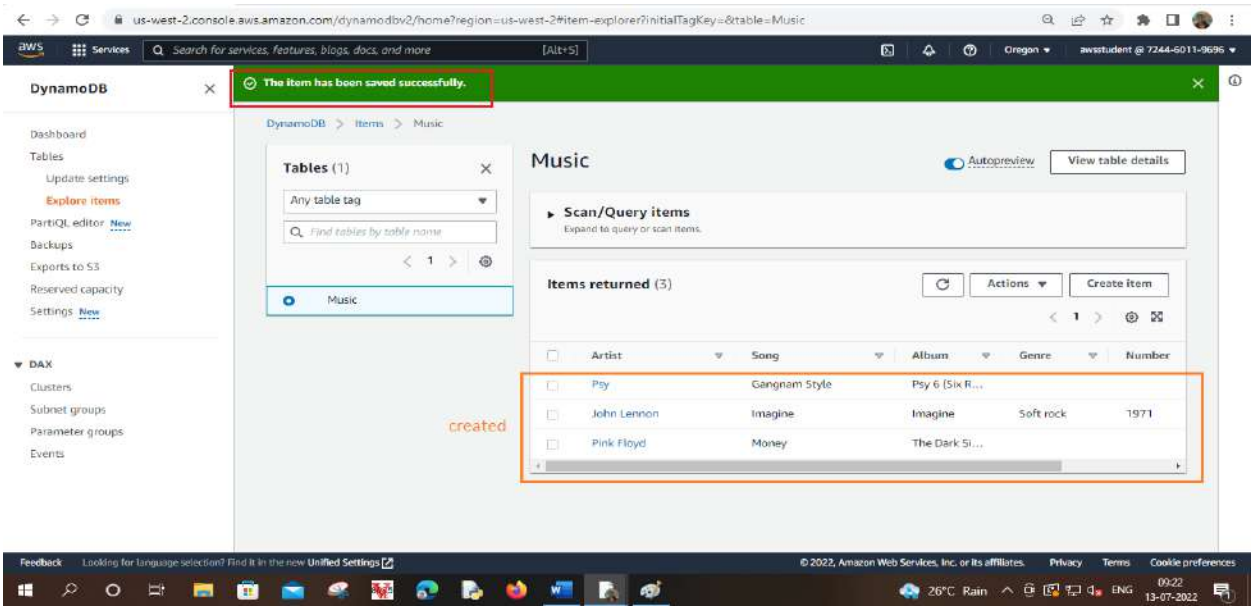




Step 22 – Now create a third Item, using these attributes.

Attribute Name	Attribute Type	Attribute Value
Artist	String	Psy
Song	String	Gangnam Style
Album	String	Psy 6 (Six Rules), Part 1
Year	Number	2011
LengthSeconds	Number	219





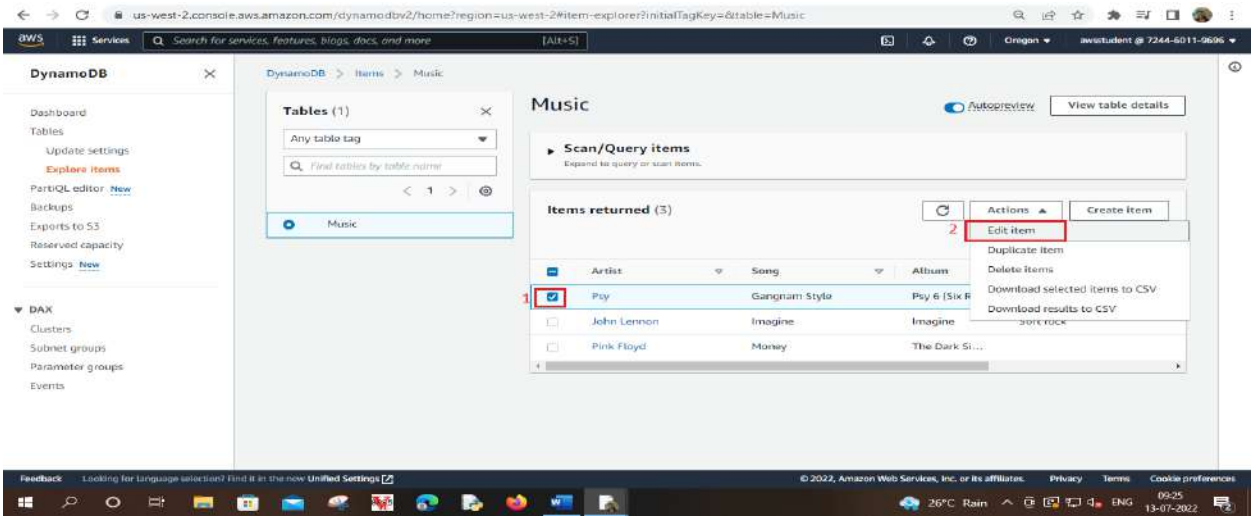
Once again, this item has a new Length Seconds attribute identifying the length of the song. This demonstrates the flexibility of a NoSQL database.

There are also faster ways to load data into DynamoDB, such as using AWS Data Pipeline, programmatically loading data or using one of the free tools available on the Internet.

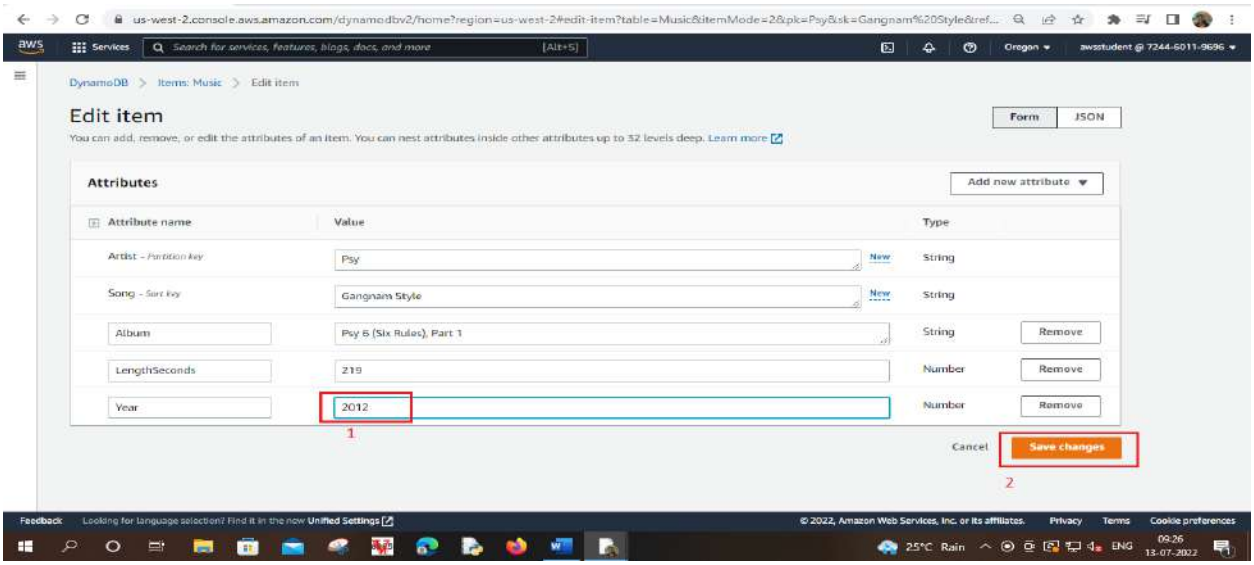
Task 3: Modify an Existing item

You now notice that there is an error in your data. In this task, you will modify an existing item.

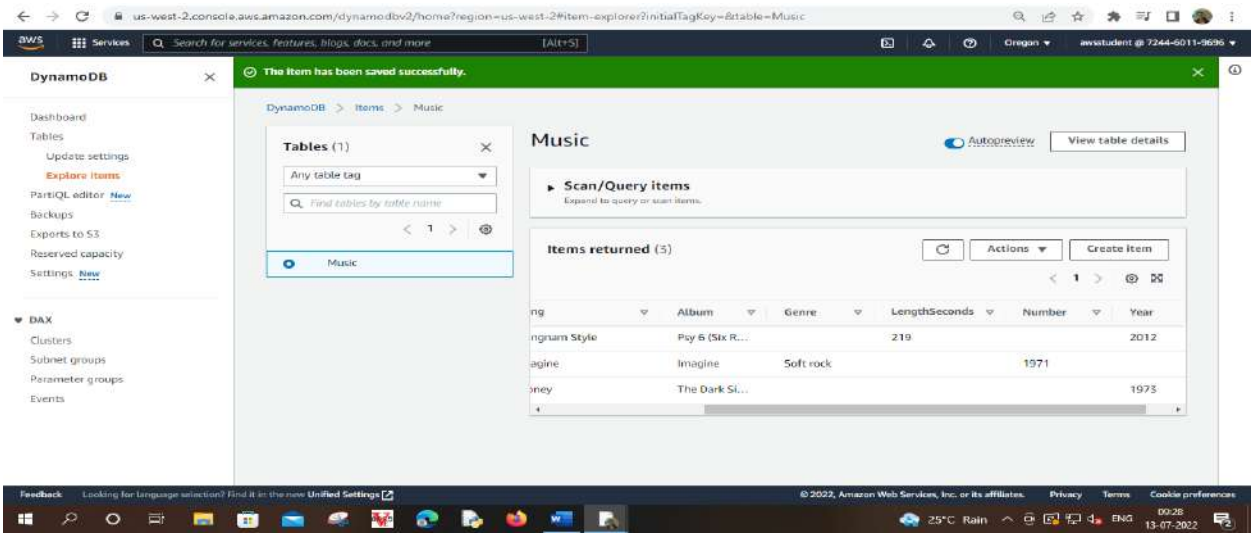
Step 23 – Choose **Psy**.

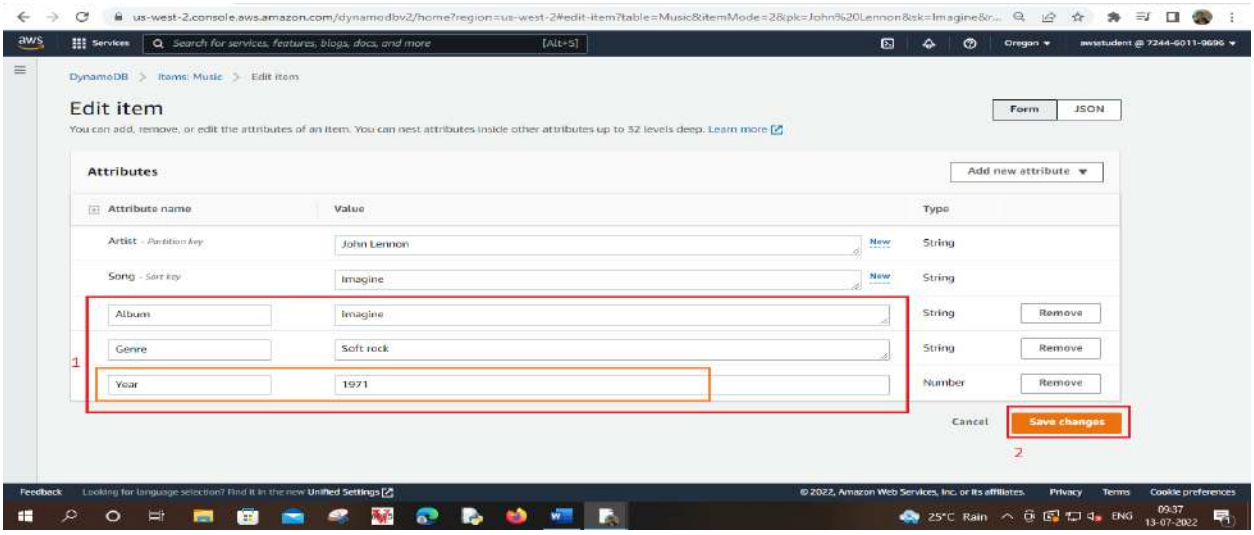


Step 24 – Change the Year from 2011 to 2012.

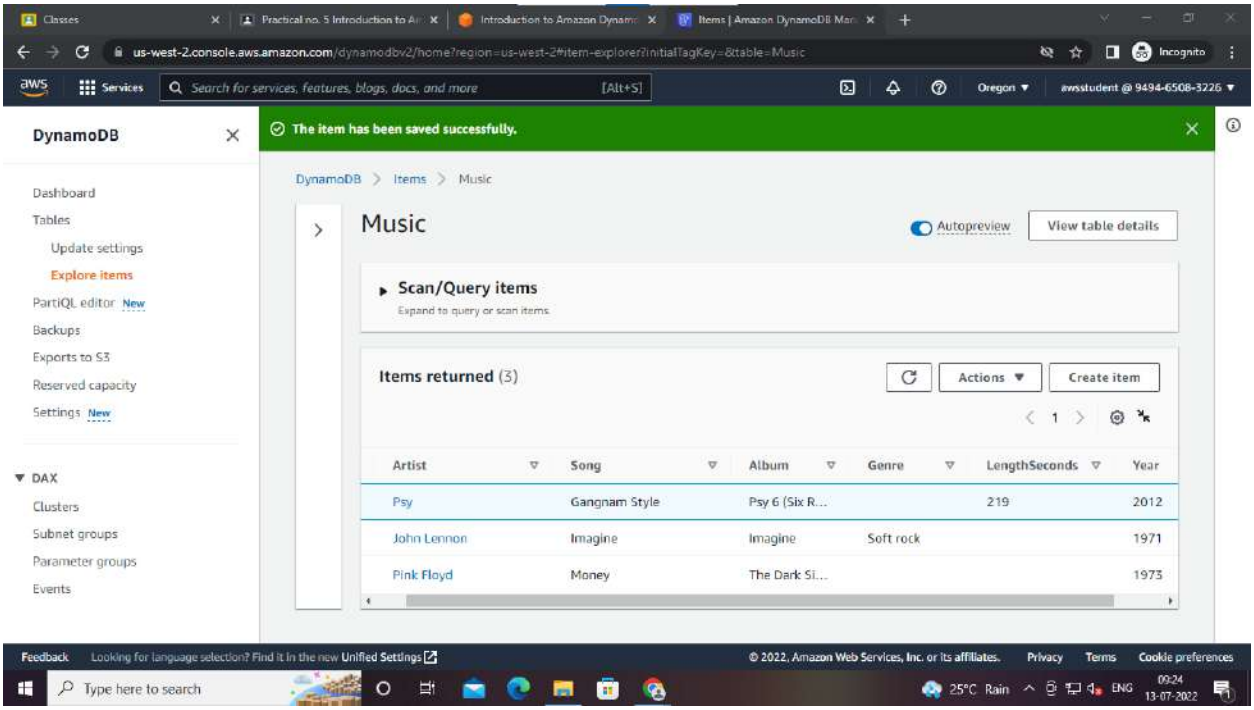


Step 25 – Choose Save changes.





The item is now updated.

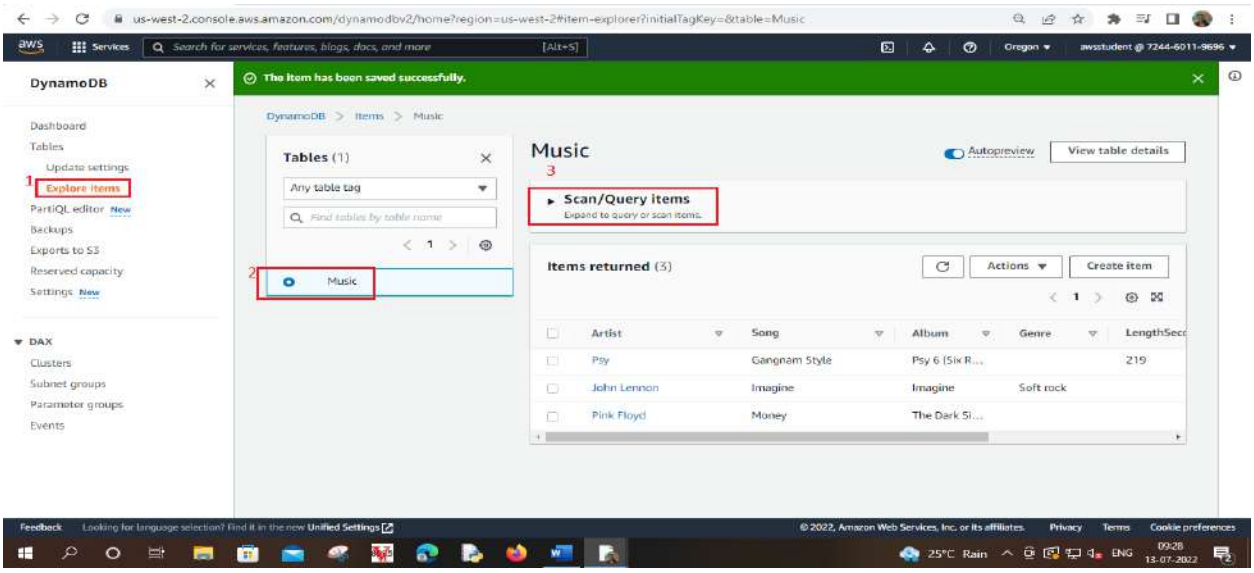


Task 4: Query the Table

There are two ways to query a DynamoDB table: Query and scan.

A **query** operation finds items based on Primary Key and optionally Sort Key. It is fully indexed, so it runs very fast.

Step 26 – In the left navigation pane, choose **Explore items**.



Step 27 – Choose **Music.**

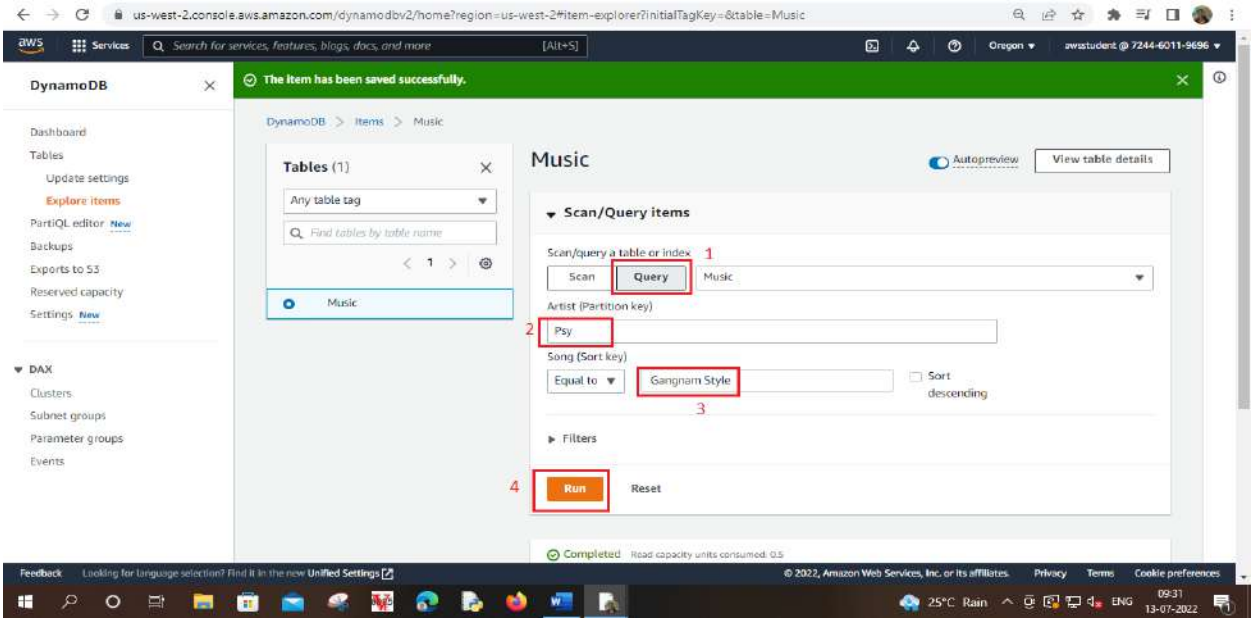
Step 28 – Expand > **Scan/Query items** to query or scan items.

Step 29 – Choose **Query.**

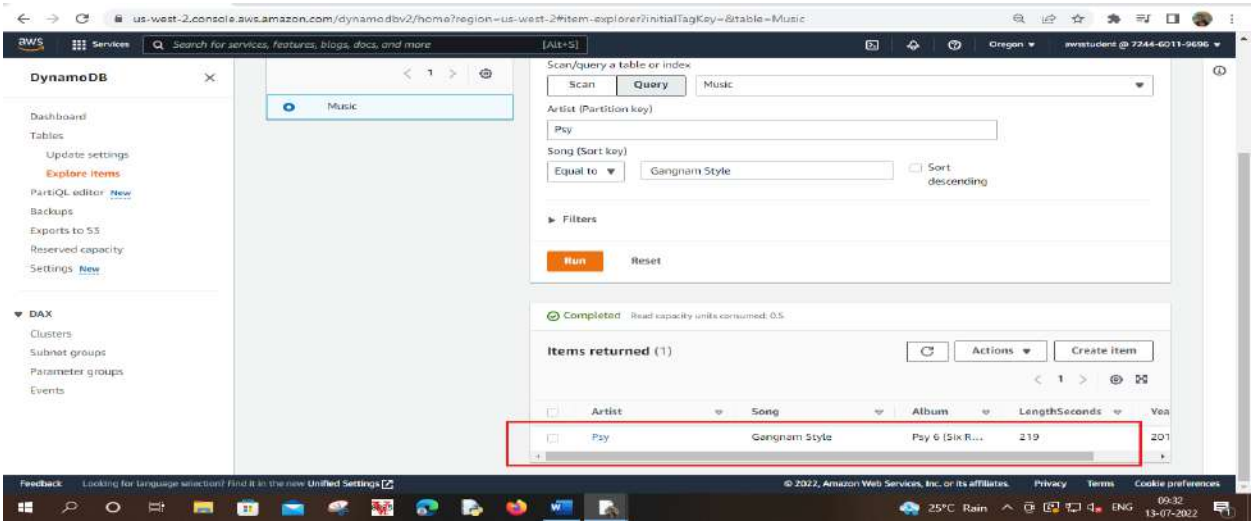
Fields for the Partition Key (which is the same as Primary Key) and Sort Key are now displayed.

Step 30 – Enter these details.

- **Artist (Partition Key):** Psy
- **Song (Sort Key):** Gangnam Style



Step 31 – Choose Run.

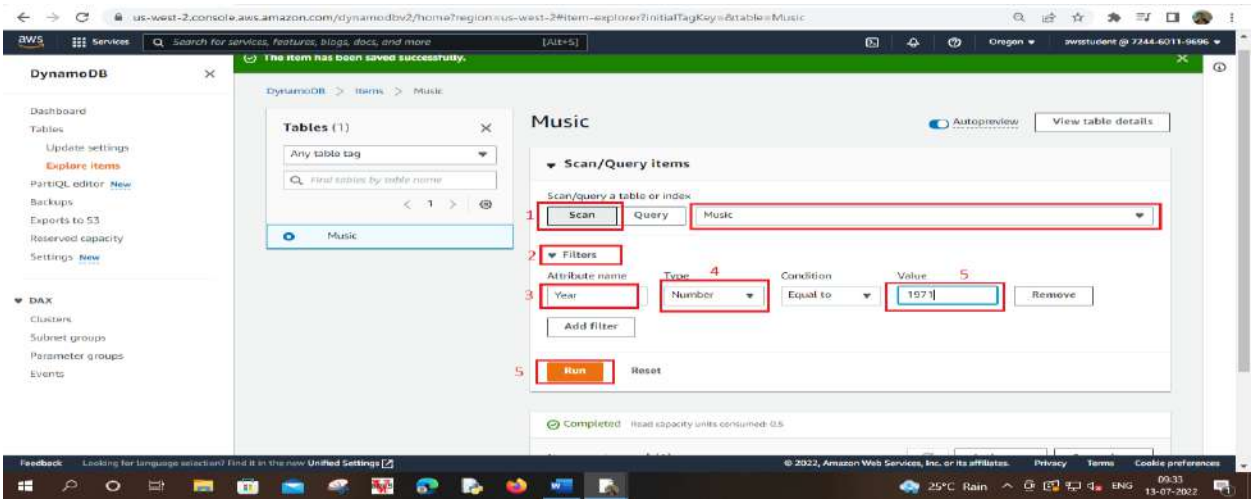


The song quickly appears in the list. A query is the most efficient way to retrieve data from a DynamoDB table.

Alternatively, you can scan for an item. This involves looking through every item in a table, so it is less efficient and can take significant time for larger tables.

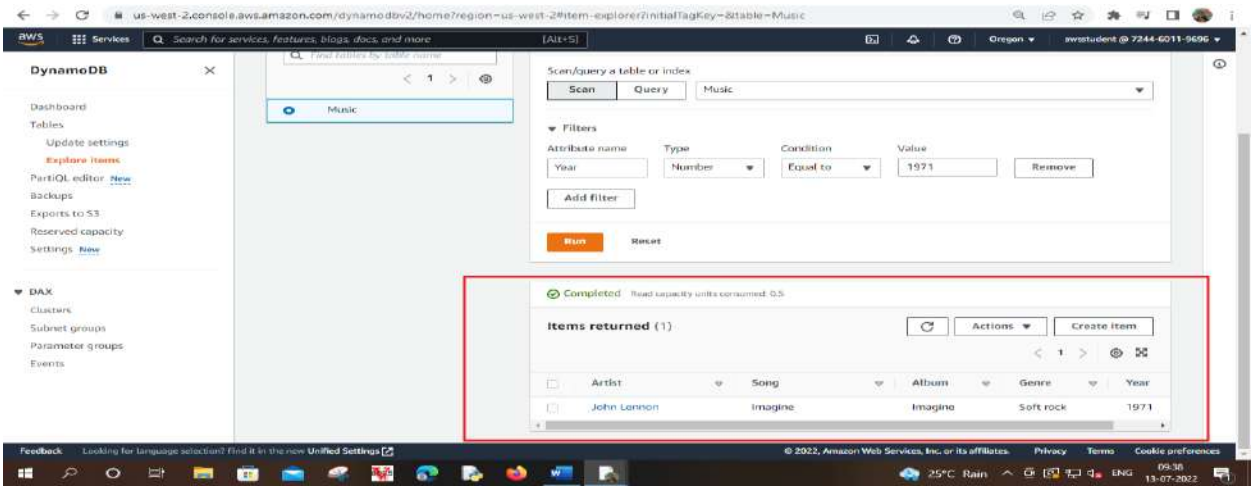
Step 32 – Choose Scan, then expand the filters, then use this filter.

- **Attribute Name:** Year
- **Type:** Number
- **Value:** 1971



Step 33 – Choose Run.

Only the song released in 1971 is displayed.



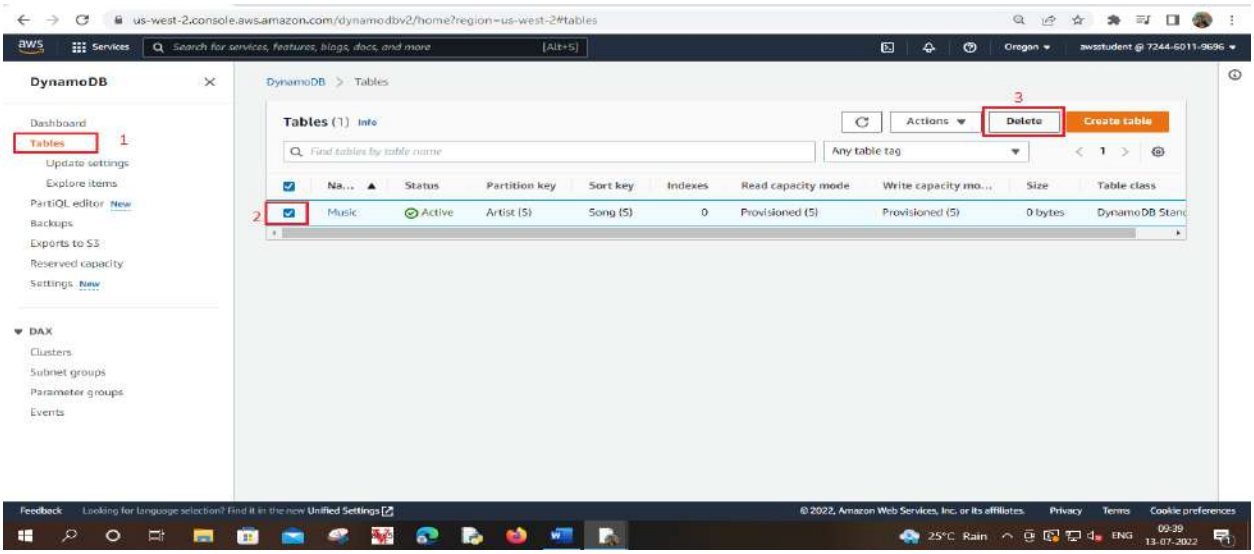
Task 5: Delete the Table

In this task, you will delete the Music table, which will also delete all the data in the table.

Step 34 – In the left navigation pane, choose **Tables**.

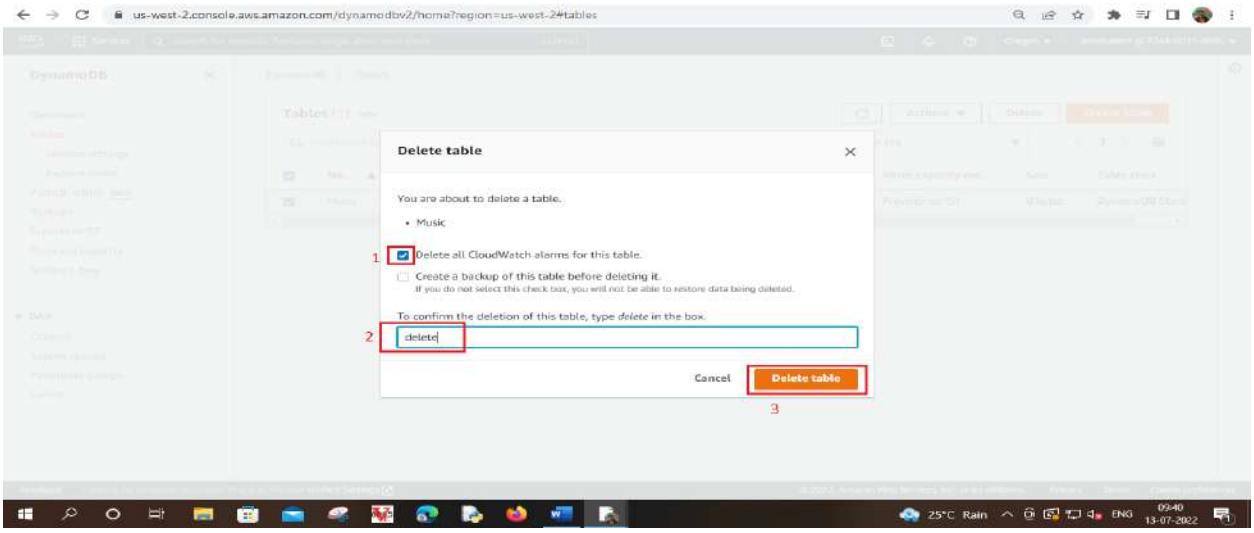
Step 35 – Choose the **Music** Tables.

Step 36 – Choose **Delete**.

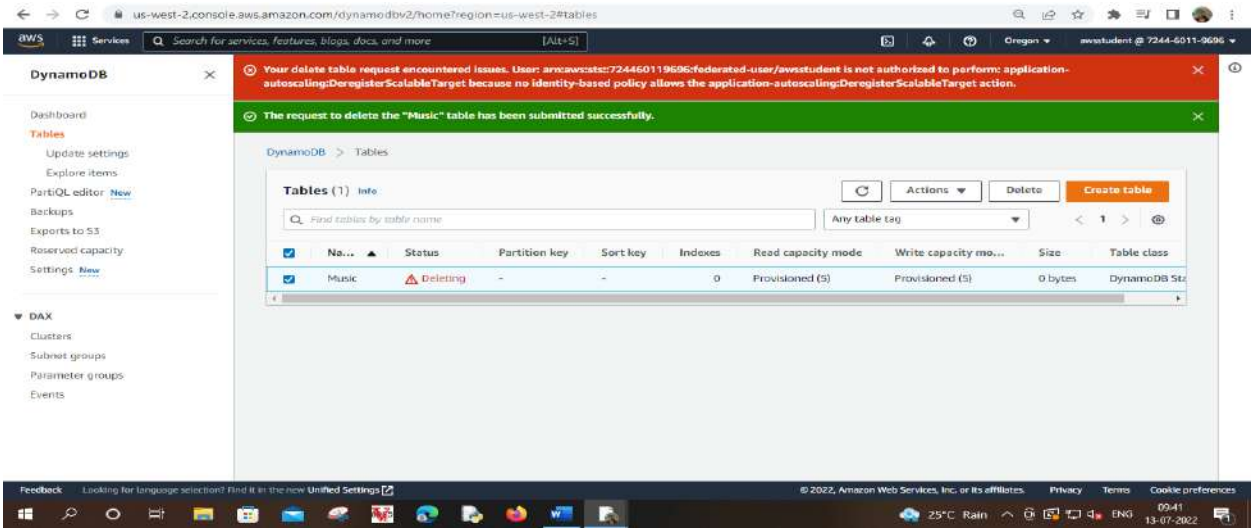


Step 37 – Enter delete.

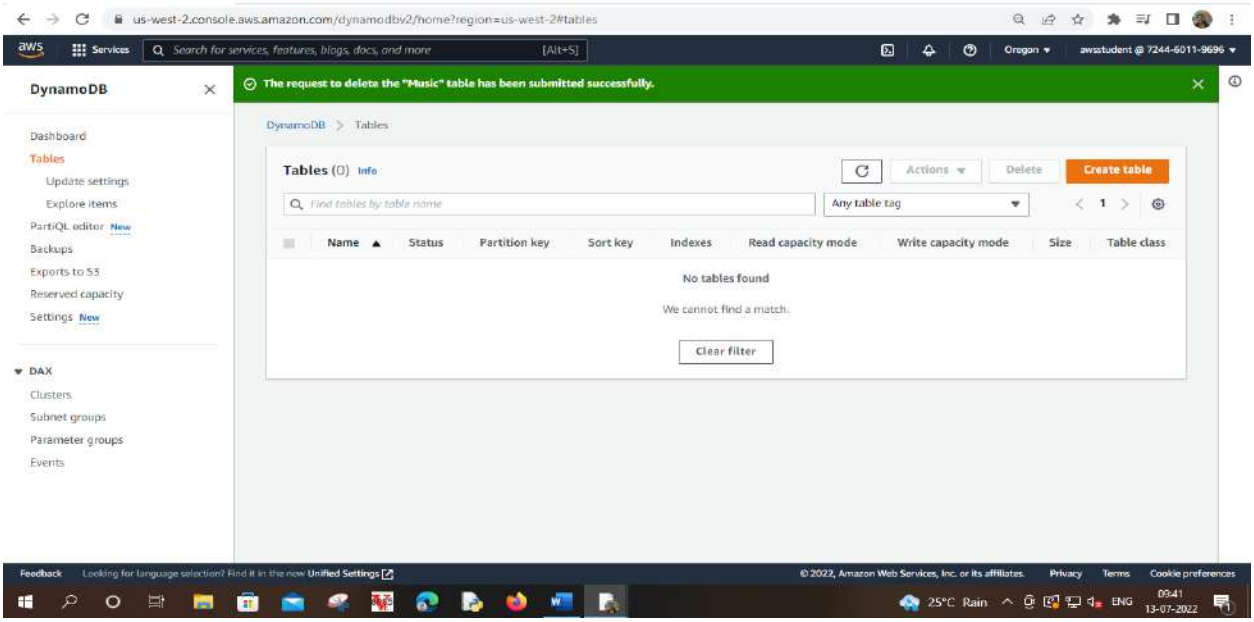
Step 38 – Choose delete table.



The table will be deleted.



Successfully deleted



Step 39 –Return to the AWS Management Console

Step 40 –At the upper-right corner of the page, choose **awsstudent@<AccountNumber>,** and then choose **Sign out.**

Step 41 –Choose **End Lab**

Practical 6: Introduction to Amazon Redshift

A. Launch an amazon redshift cluster
B. Launch Pgweb to communicate with the redshift cluster
C. Create a table
D. Load sample data from amazon S3
E. Query data

Amazon Redshift

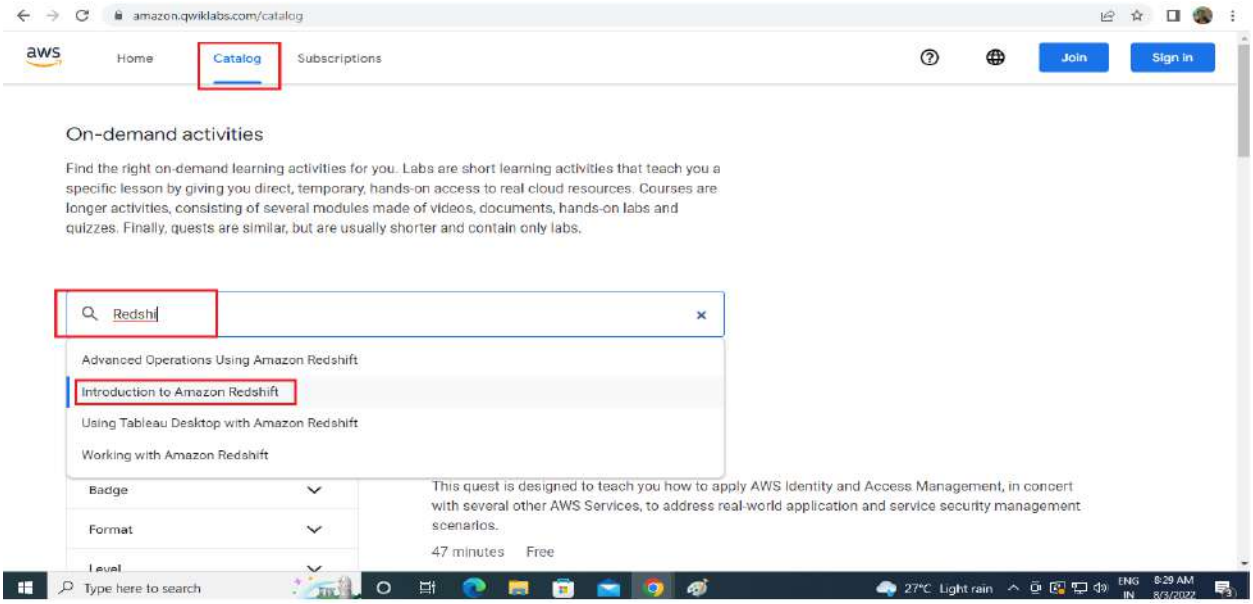
Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze all your
data using standard SQL and your existing Business Intelligence (BI) tools.
It demonstrates the basic steps required to get started with Redshift including:

1. Creating a Redshift cluster
2. Loading data into a Redshift cluster
3. Performing queries against the data in cluster

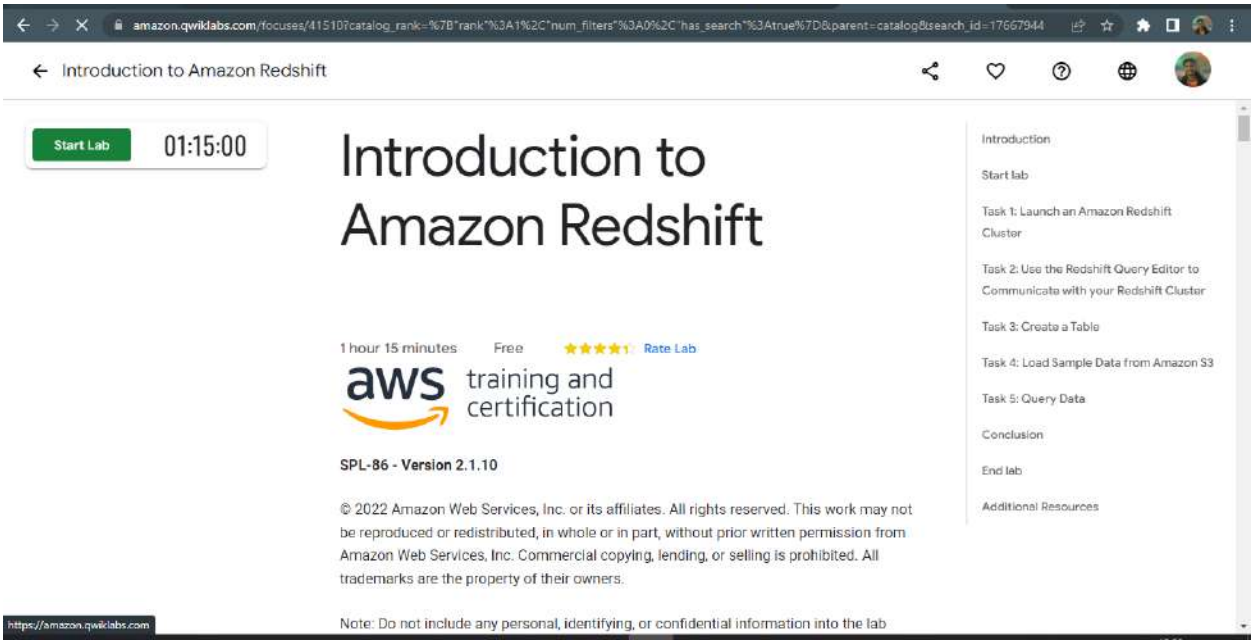
Task 1: Launch an amazon Redshift Cluster

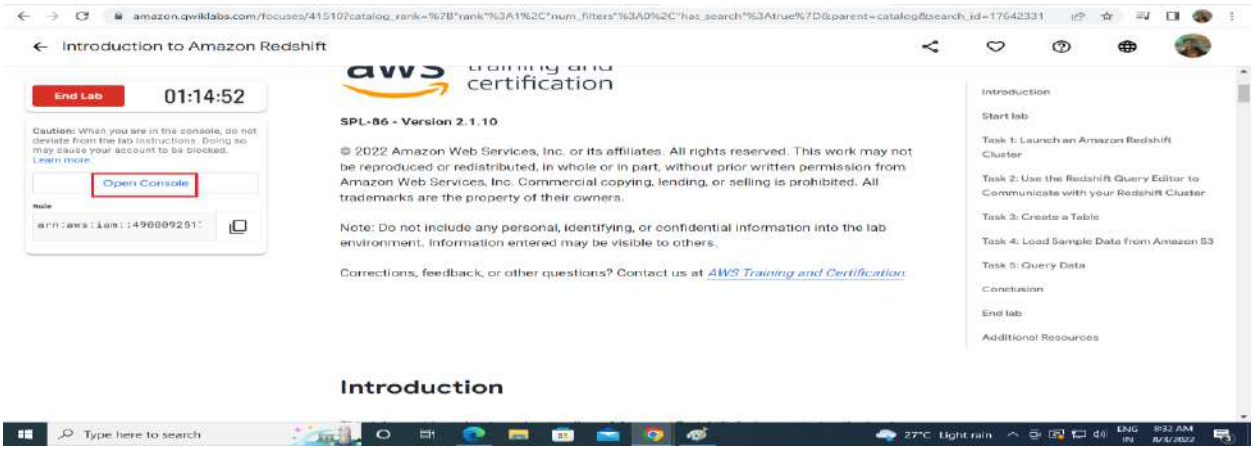
Step 1 – Go to the given link
https://amazon.qwiklabs.com/catalog

Step 2 – Search the Redshift on given search box, after that show some option then select the "Introduction to Amazon
Redshift" same like the below image

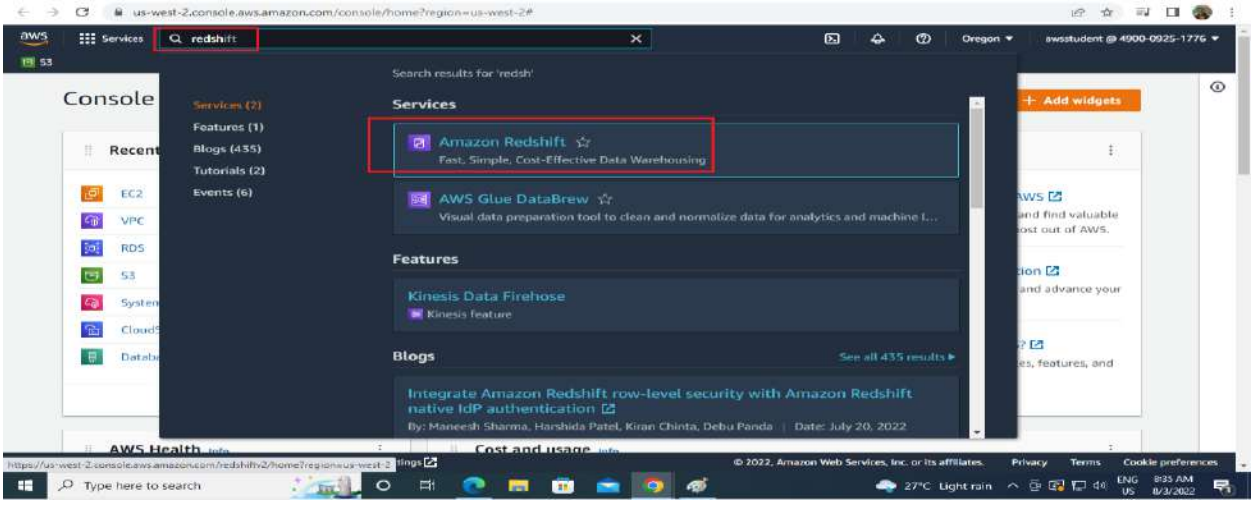


Step 3 – Start Lab and click on Open Console

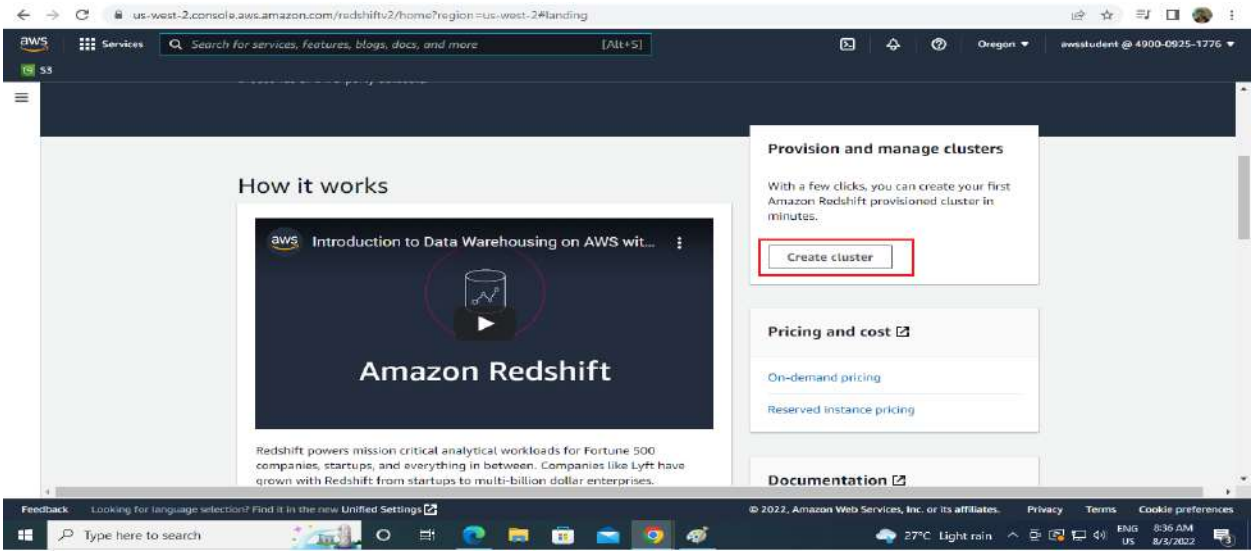




Step 4 – In the AWS Management Console, choose **Services**, then choose **Amazon Redshift.**

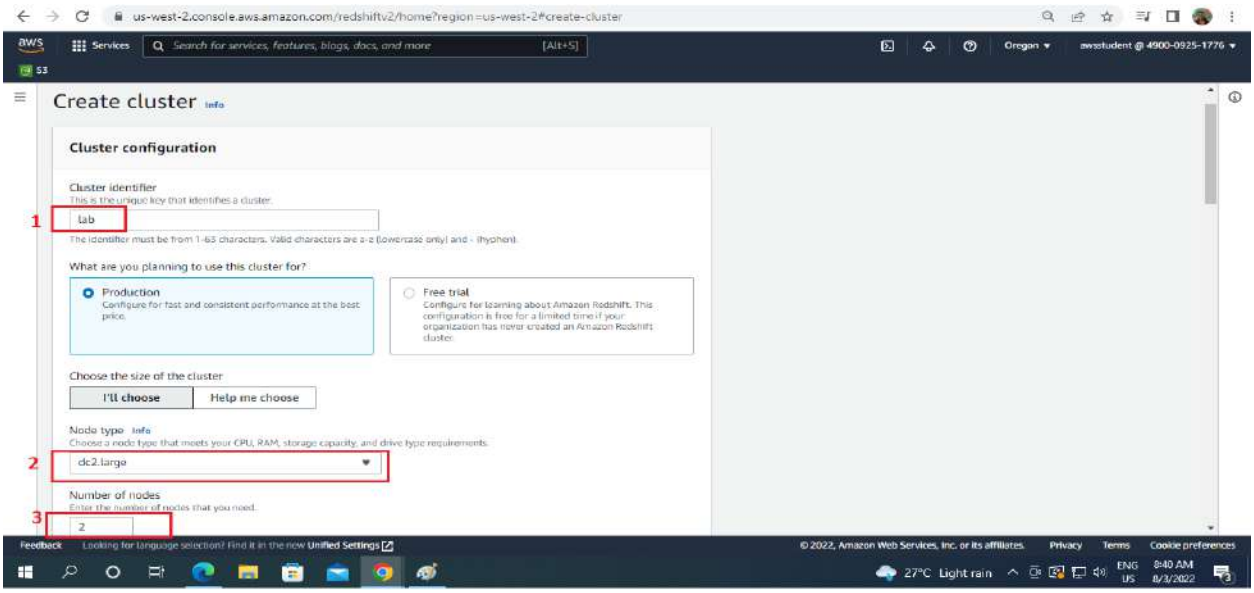


Step 5 – Choose Create cluster.



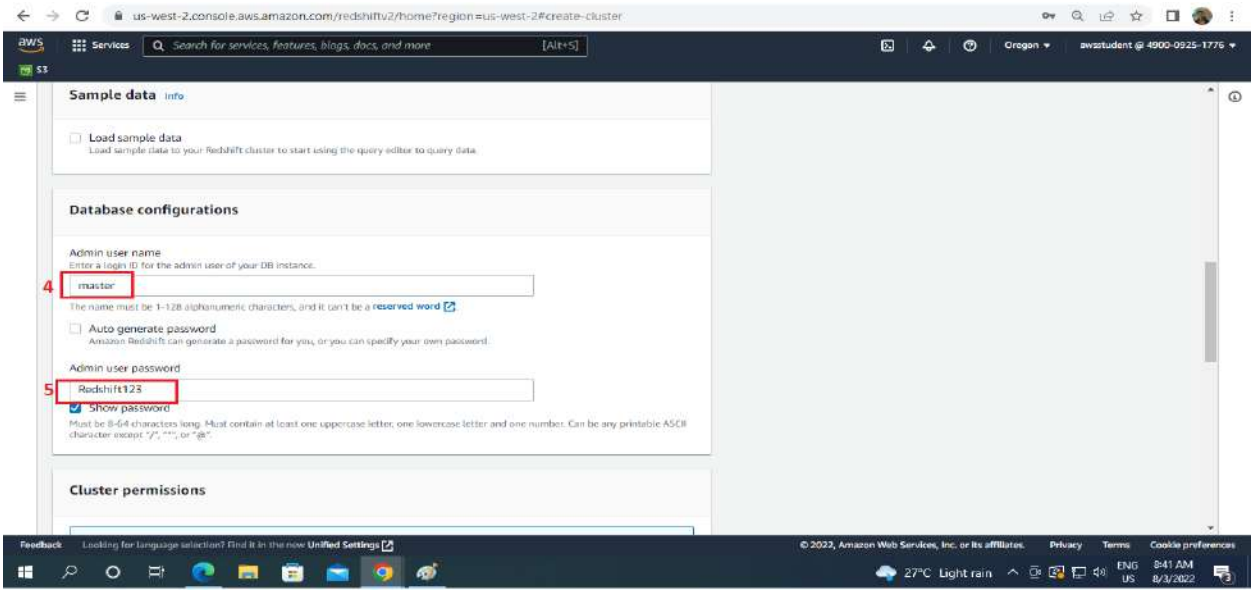
Step 6 – In the Cluster configuration section, configure:

1. Cluster identifier: **lab**
2. Node type: **dc2.large**
3. Number of nodes: **2**

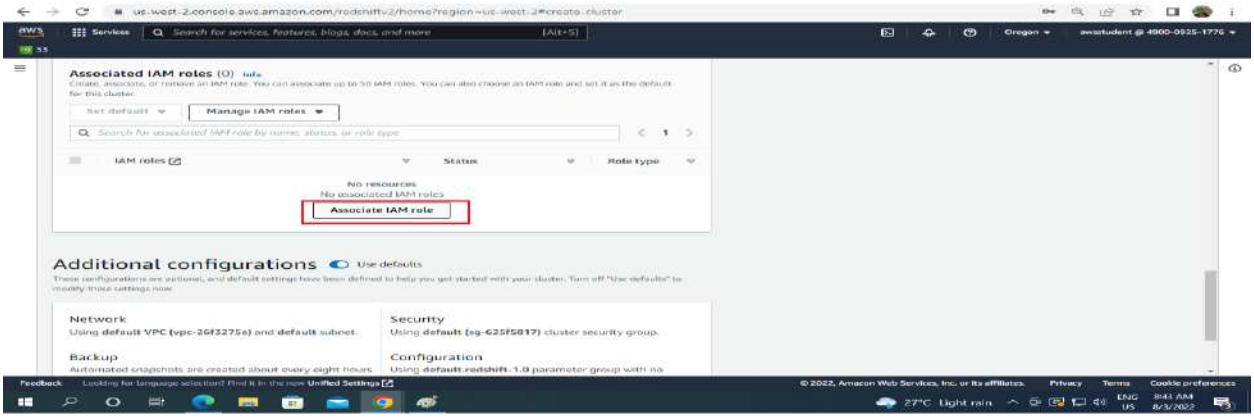


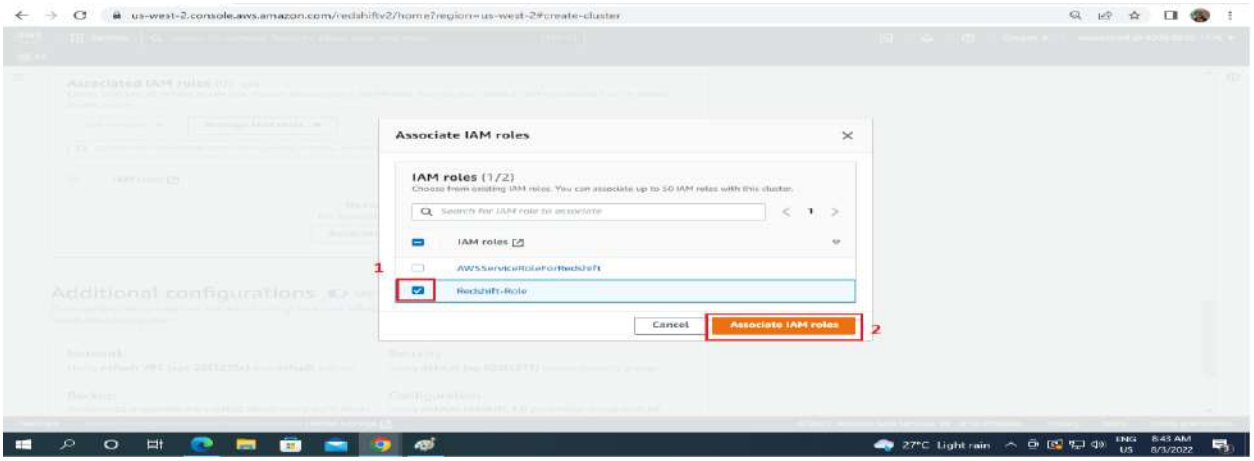
Step 7 – In the Database configurations section, configure:

1. Admin user name: **master**
2. Admin user password: **Redshift123**



Step 8 – For **Sort Key**, type Song. For **Associated IAM roles**, Click Associate IAM role button. Select the Redshift-Role and click Associated IAM Roles





The role grants permission for Amazon Redshift to read data from Amazon S3.

Step 9 – In the Additional configurations section,

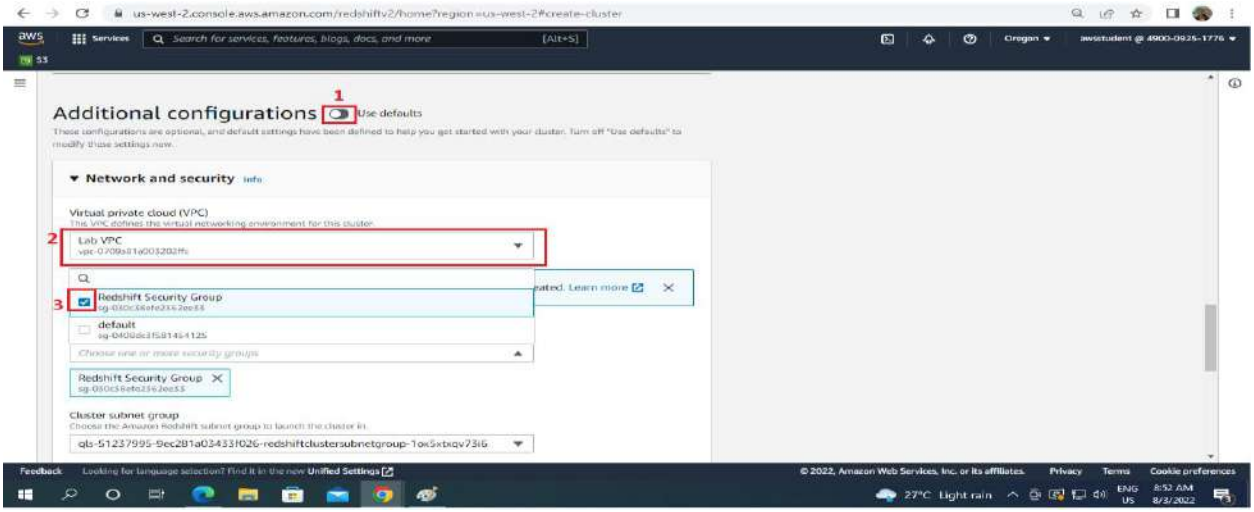
1. Deselect Use defaults

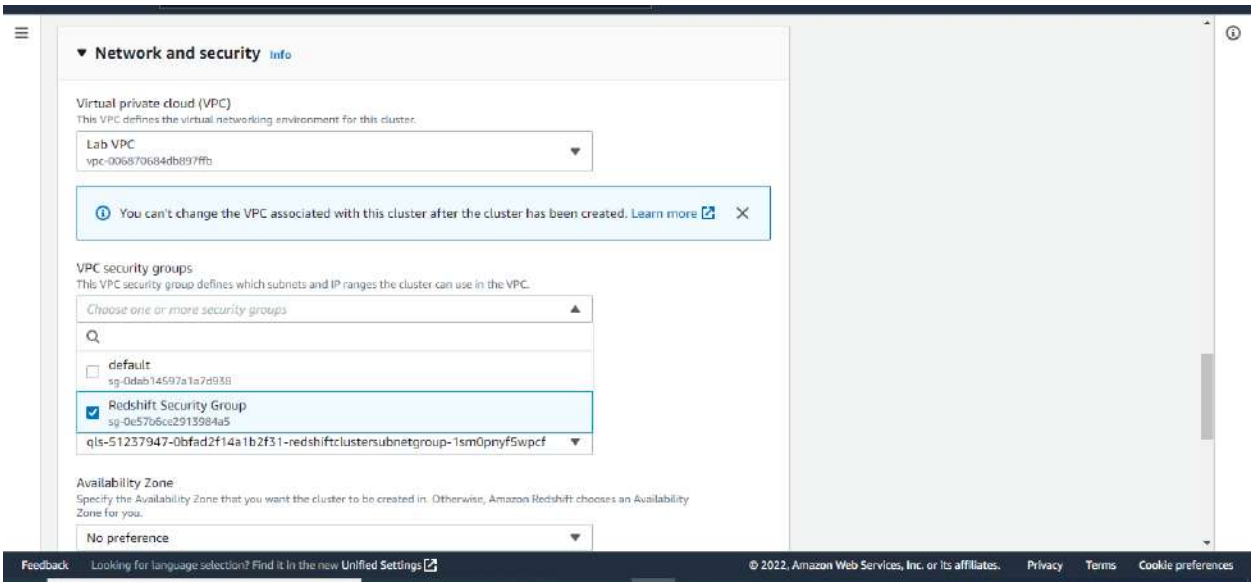
Expand Network and security, then configure:

• Virtual private cloud: Lab VPC

• VPC security groups:

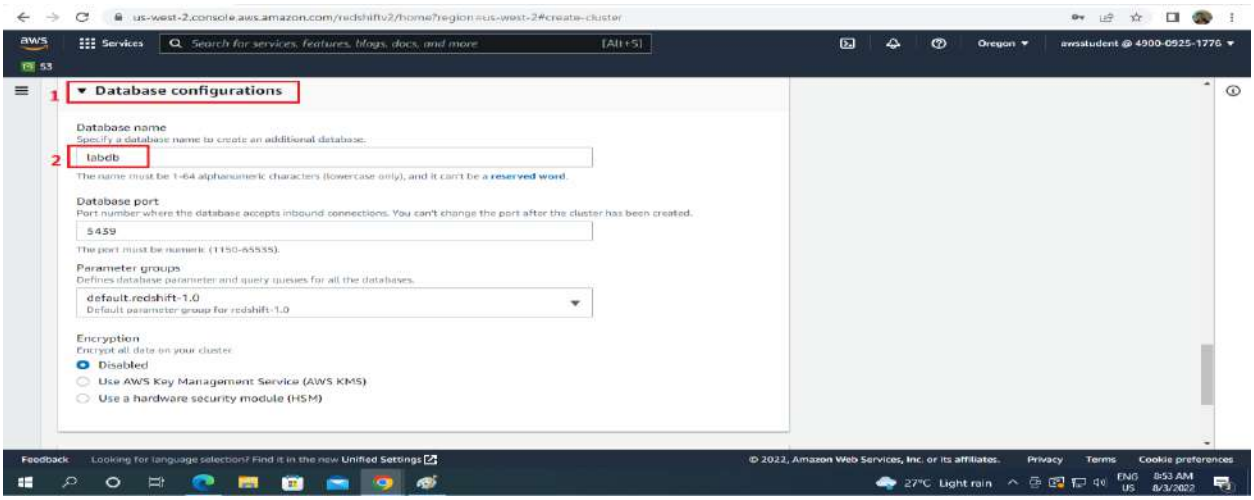
- **Deselect** Use default
- **Check or select** Redshift Security Group.



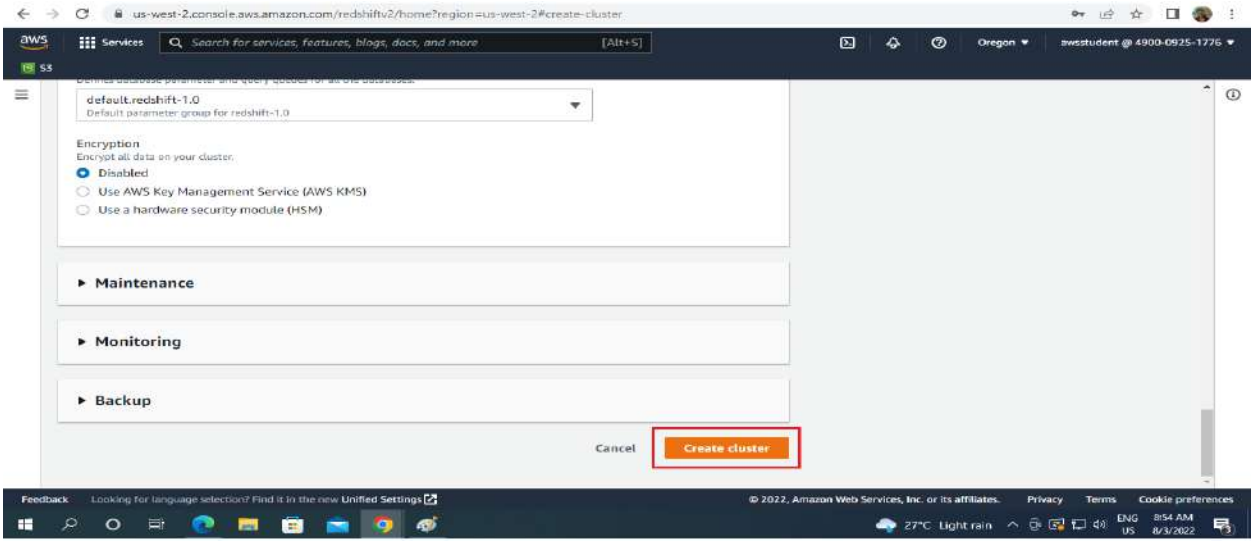


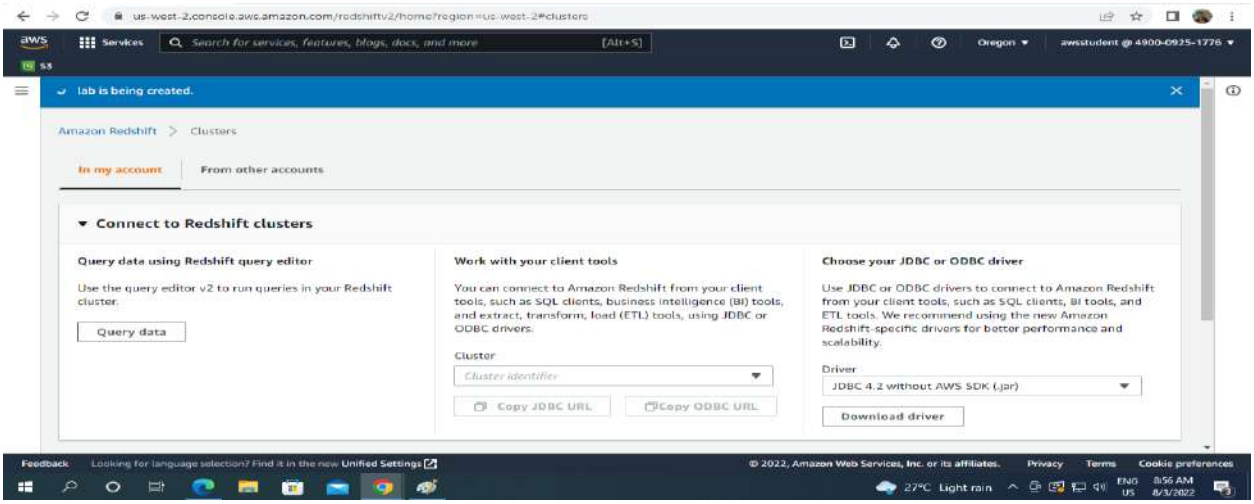
Step 10 – Expand Database configurations, then configure:

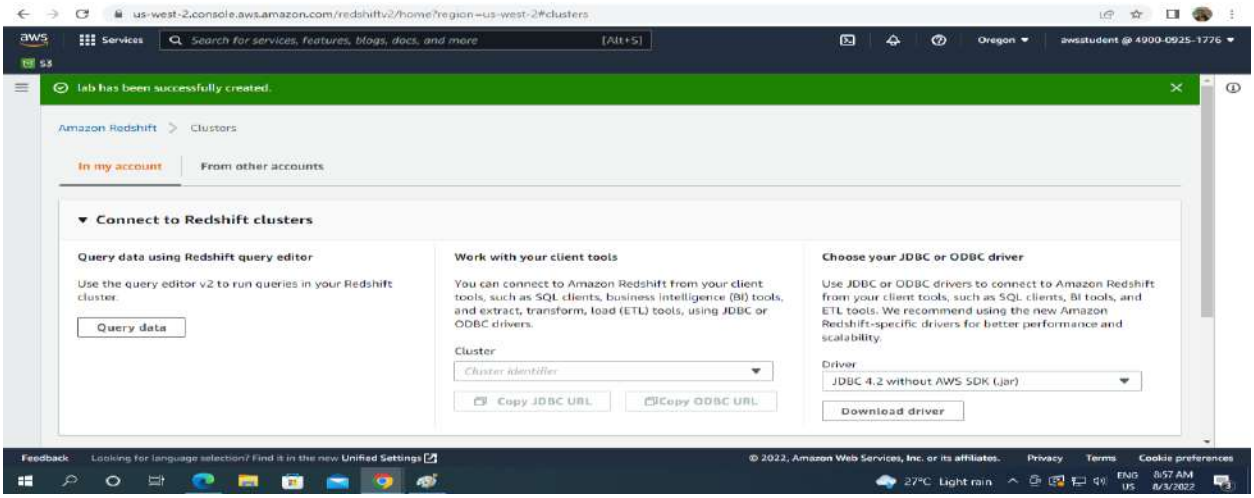
• Database name: labdb



Step 11 – Scroll to the bottom of the screen, then click **Create cluster** button.

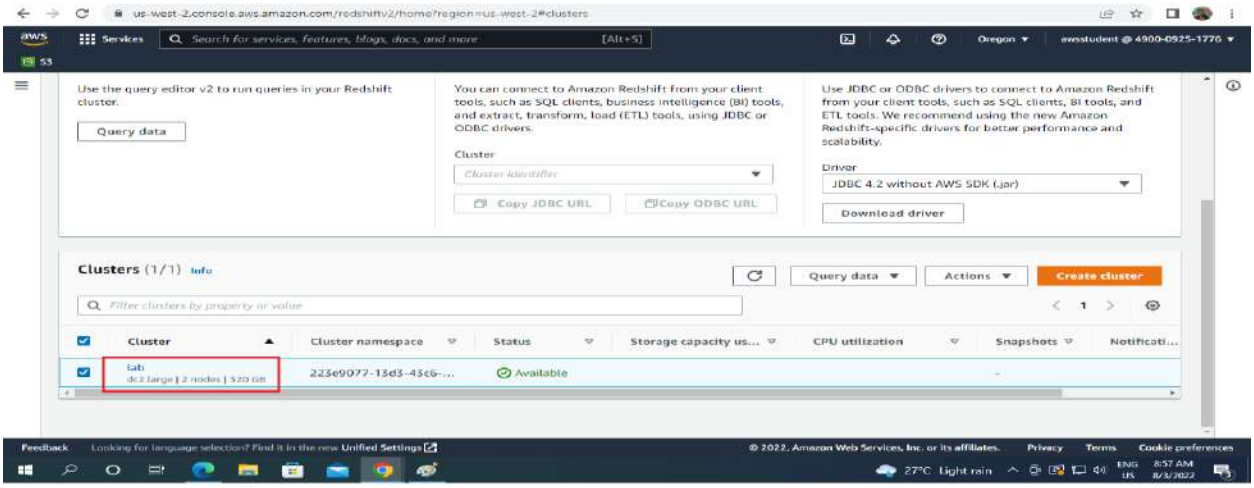




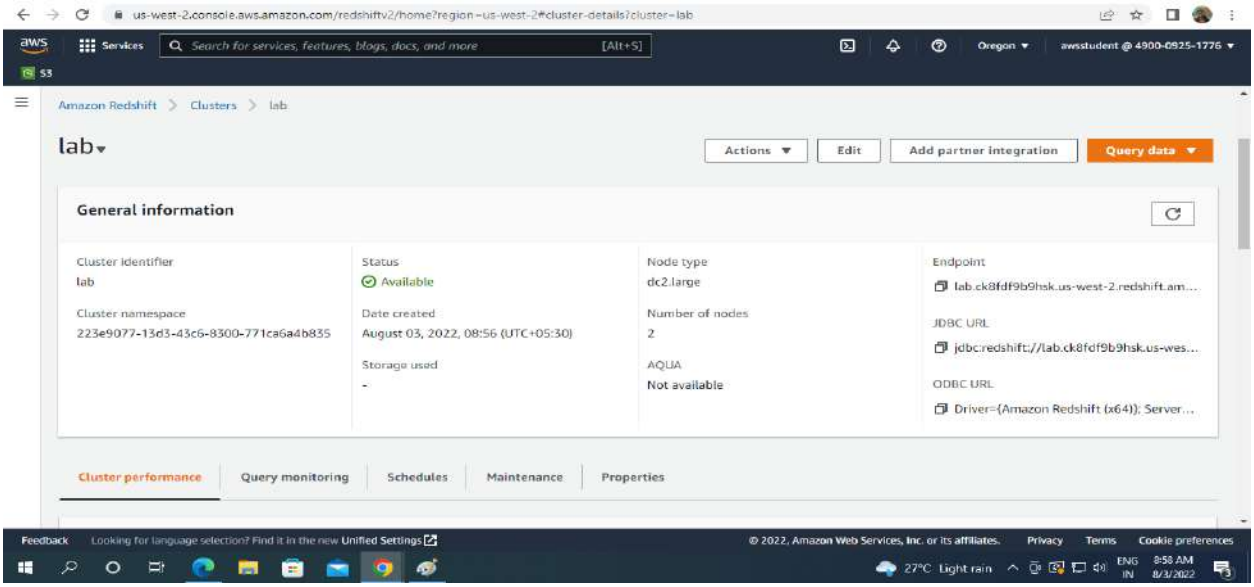


Click the name of your Cluster (**lab**)

The cluster configuration will be displayed. Spend a few minutes looking at the properties.



Wait for the Status of your cluster to display **Available** before continuing to the next task.



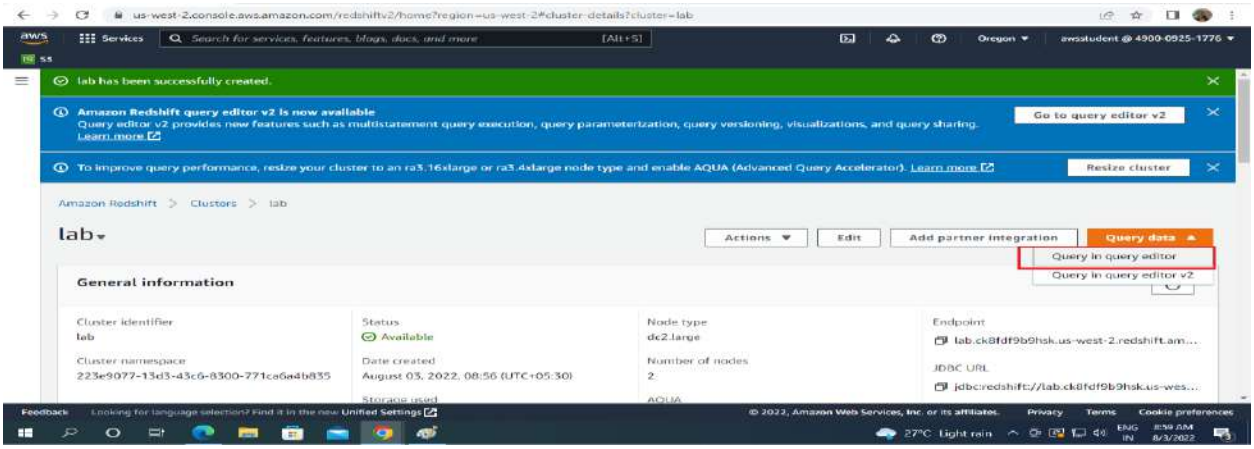
Task 2: Use the Redshift Query Editor to Communicate with your Redshift Cluster

Amazon Redshift can be used via industry-standard SQL. To use Redshift, you require an SQL Client that

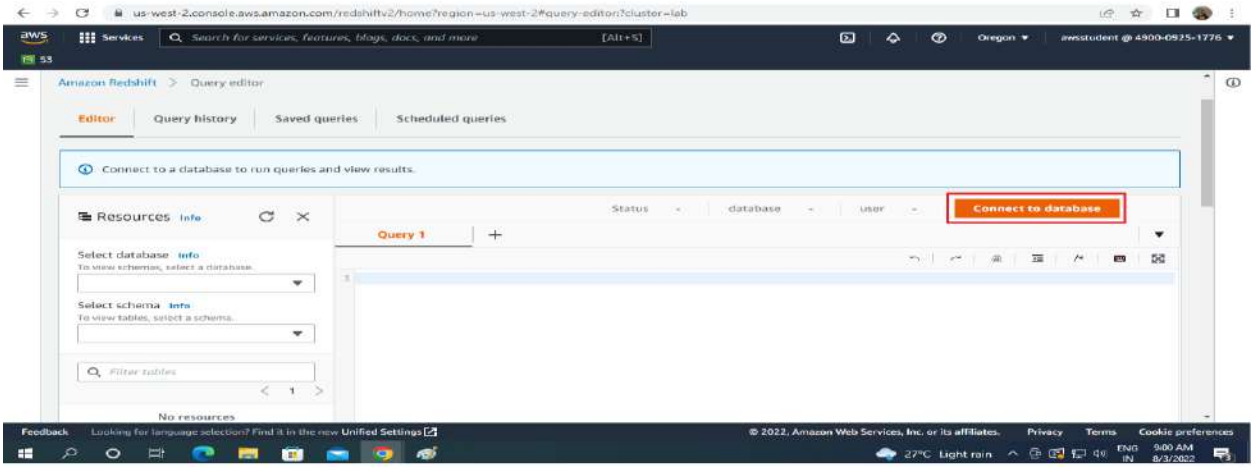
provides a user interface to type SQL. Any SQL client that supports JDBC or ODBC can be used with Redshift.

Step 12 – In the left navigation pane, click Query editor, then select Connect to database then configure:

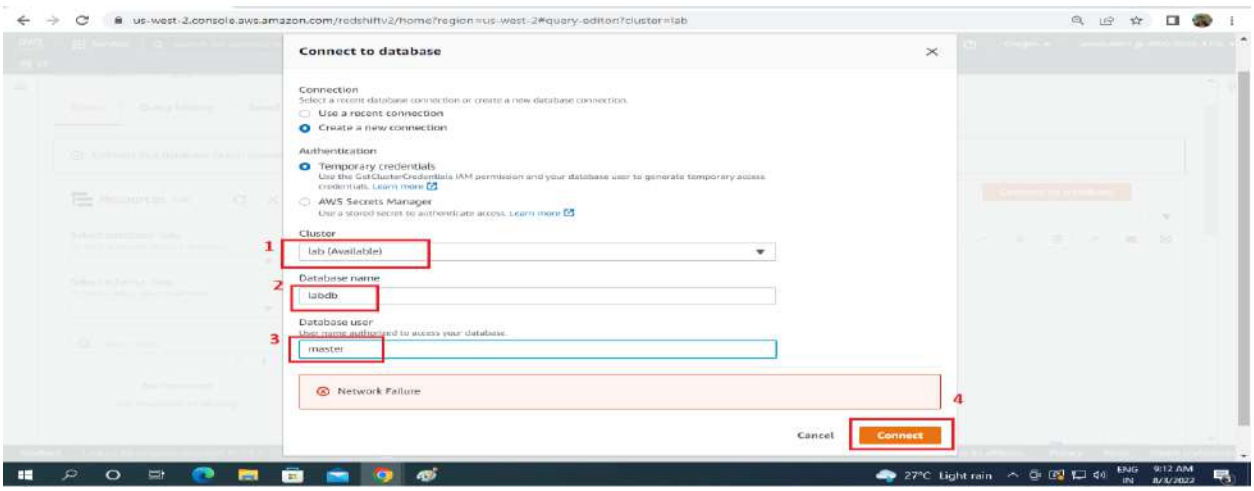
- **Cluster**: lab
- **Database name:** labdb
- **Database user:** masterStep



Step 13 – Click **Connect to database**

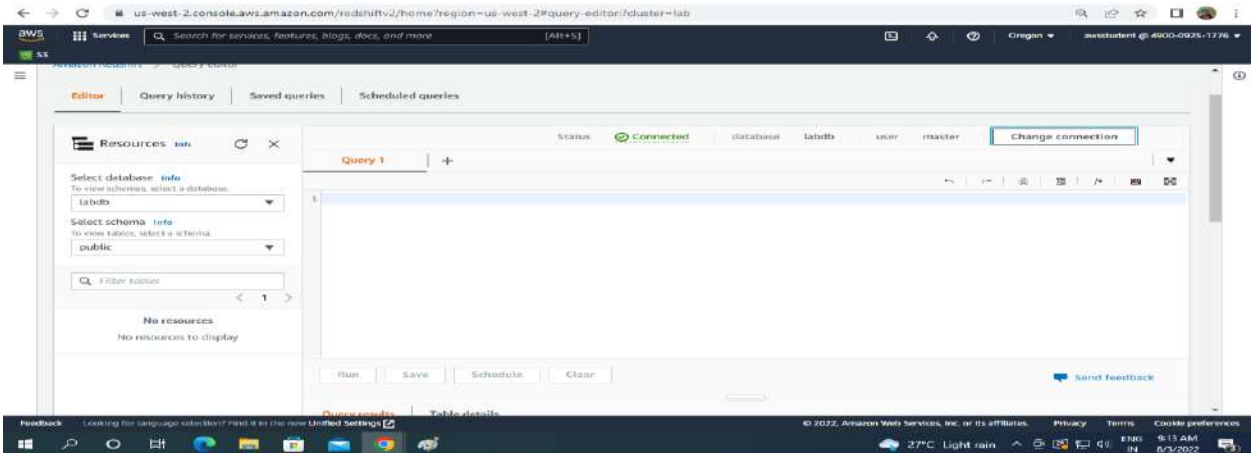


Step 14 – Click **Connect** button.

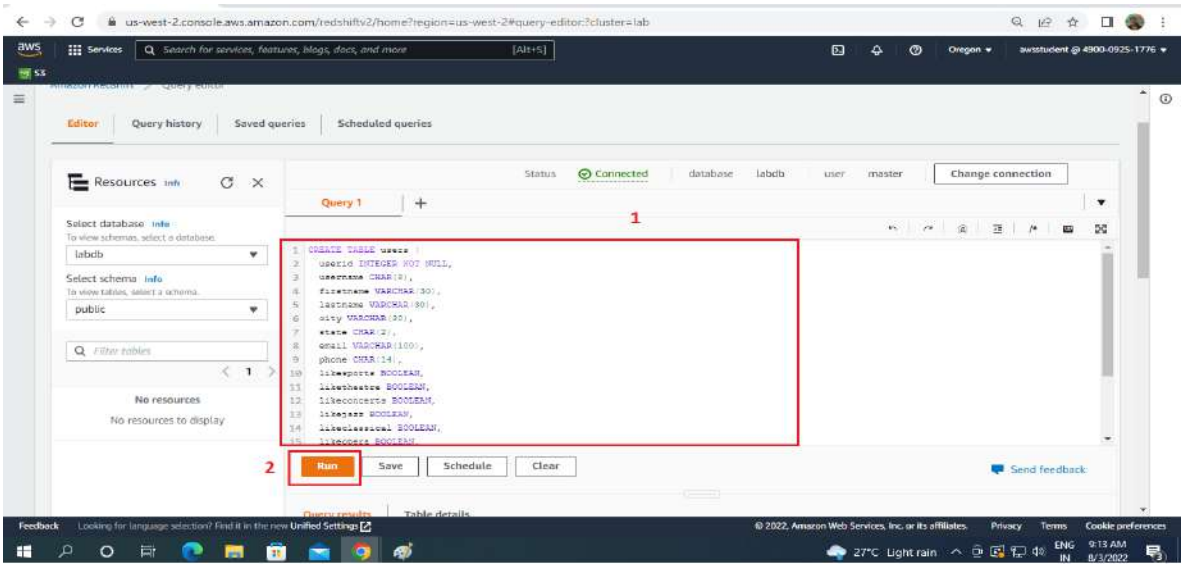


Task 3: Create a Table

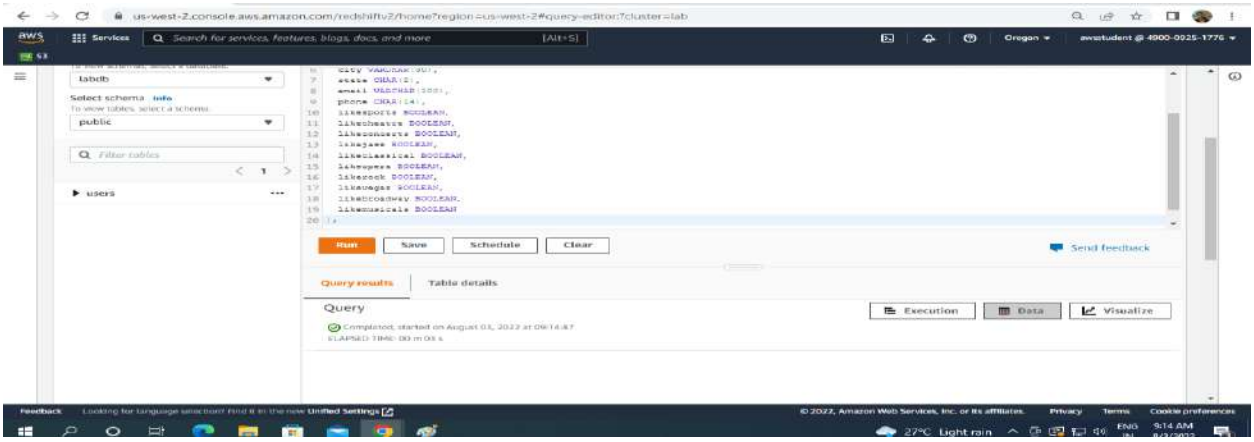
Step 15 – Copy this SQL command and paste it into the Query 1 window, then click

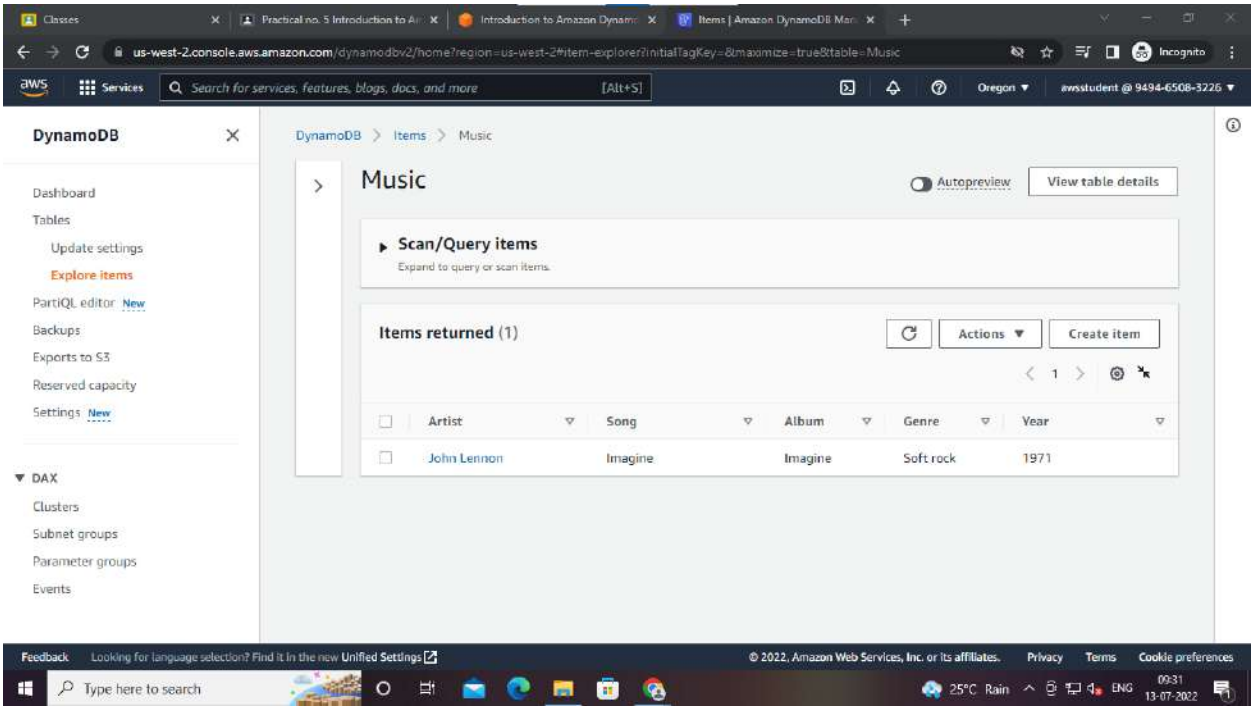



```
CREATE TABLE users (
userid INTEGER NOT NULL, username CHAR(8), firstname VARCHAR(30), lastname VARCHAR(30),
city VARCHAR(30), state CHAR(2), email VARCHAR(100), phone CHAR(14),
likesports BOOLEAN,
liketheatre BOOLEAN,
likeconcerts BOOLEAN,
likejazz BOOLEAN,
likeclassical BOOLEAN,
likeopera BOOLEAN,
likerock BOOLEAN,
likevegas BOOLEAN,
likebroadway BOOLEAN,
likemusicals BOOLEAN
);
```



This command will create a table called users. It contains name, address and details about the type of music that the user likes.





Task 4: Load Sample Data from Amazon S3

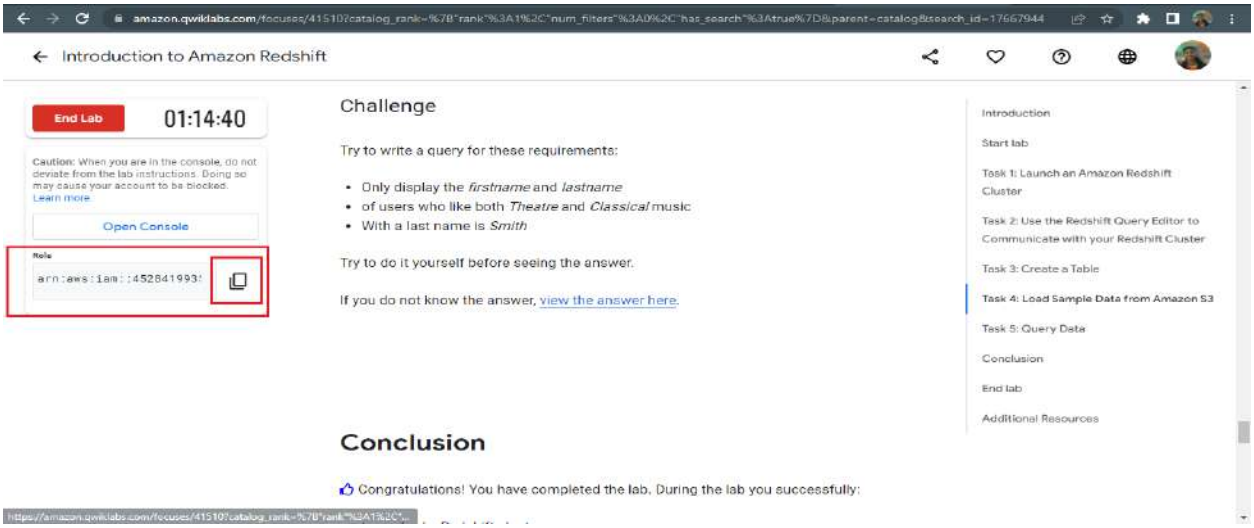
Amazon Redshift can import data from Amazon S3. Various file formats are supported, fixed-length fields, comma- separated values (CSV) and custom delimiters. The data for this lab is pipe-separated (|) ...

Step 16 – Delete the existing query, then paste this SQL command into the Query 1 window.

```
COPY users FROM 's3://awssampledbuswest2/tickit/allusers_pipe.txt' CREDENTIALS 'aws_iam_role=YOUR-ROLE' DELIMITER '|';
```

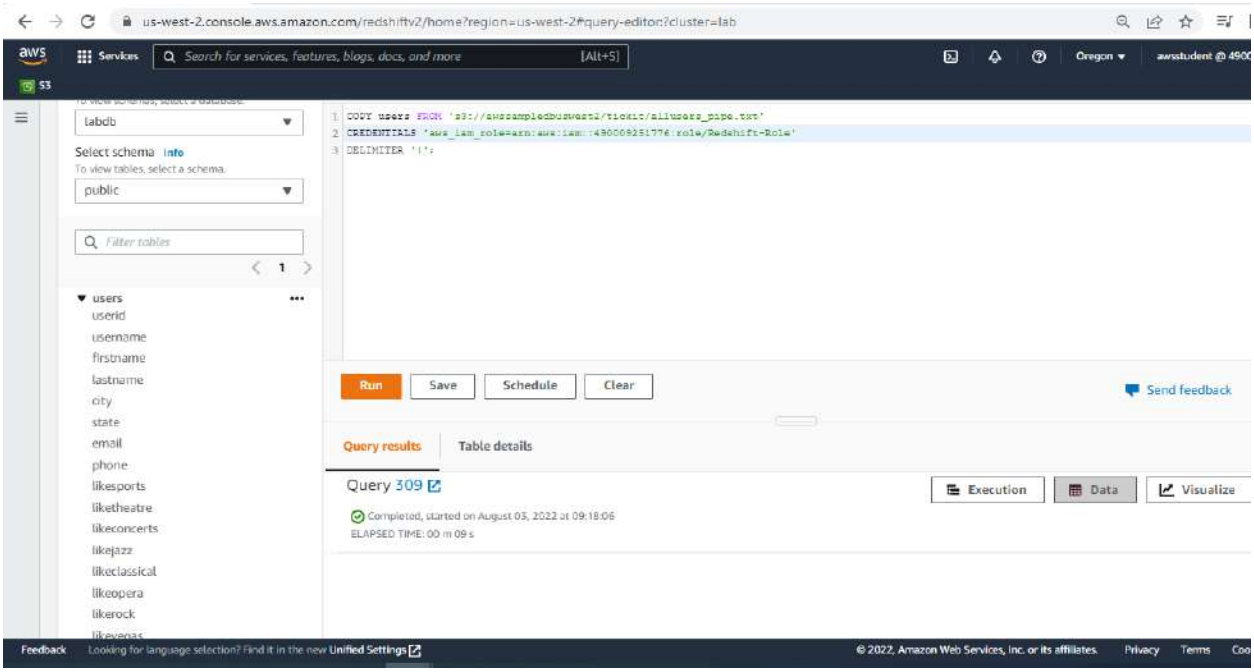
Before running this command, you will need to insert the ROLE that Redshift will use to access Amazon S3.

Step 17 – To the left of the instructions you are currently reading, copy the value for Role. It will start with: arn:aws:iam::



Step 18 – Paste the Role into the query window, replacing the text YOUR-ROLE.

Step 19 – Click Run button



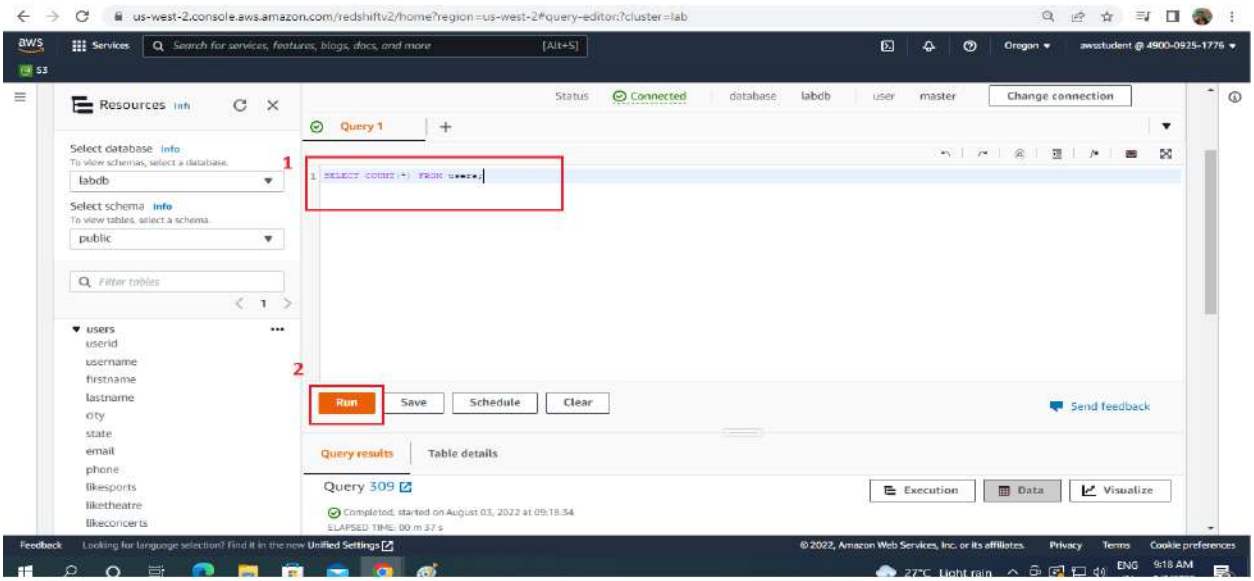
Task 5: Query Data

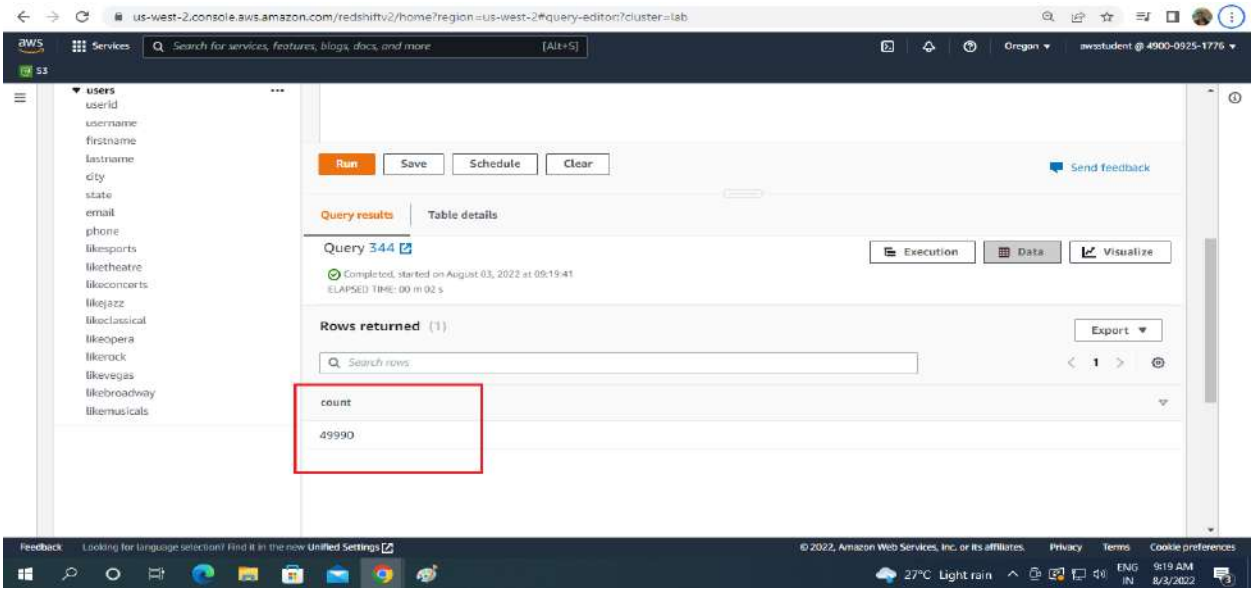
Now that you have data in your Redshift database you can query the data using SQL select statements and queries.

If you are familiar with SQL, feel free to try additional commands to query the data.

Step 20 – Run this query to count the number of rows in the user's table:

```
SELECT COUNT(*) FROM users;
```

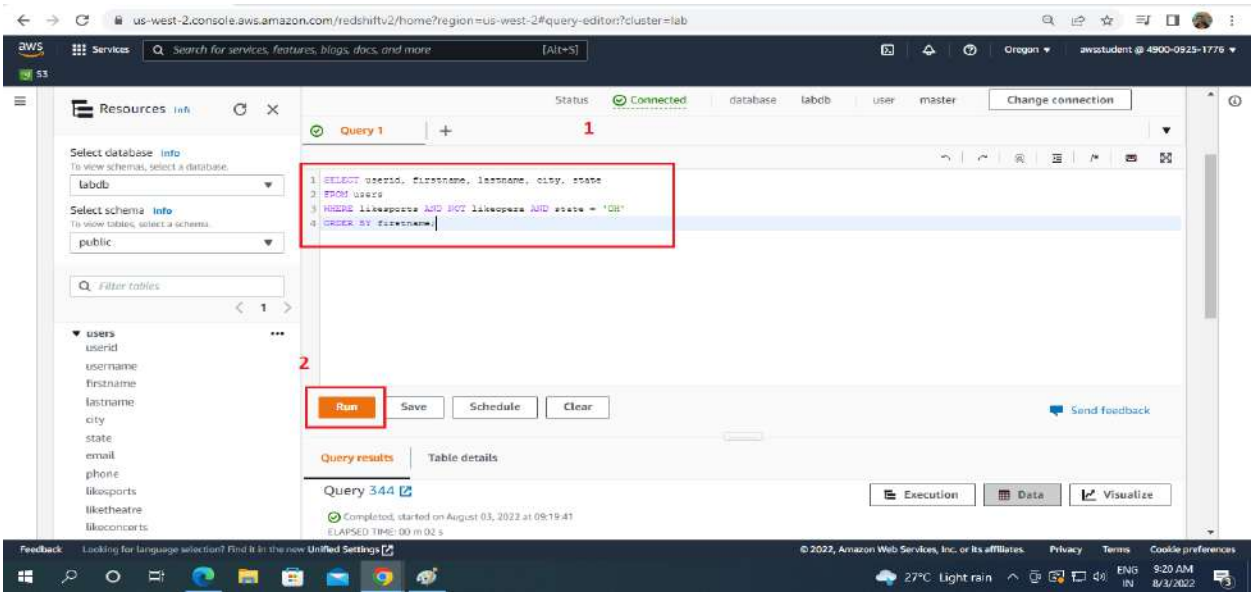




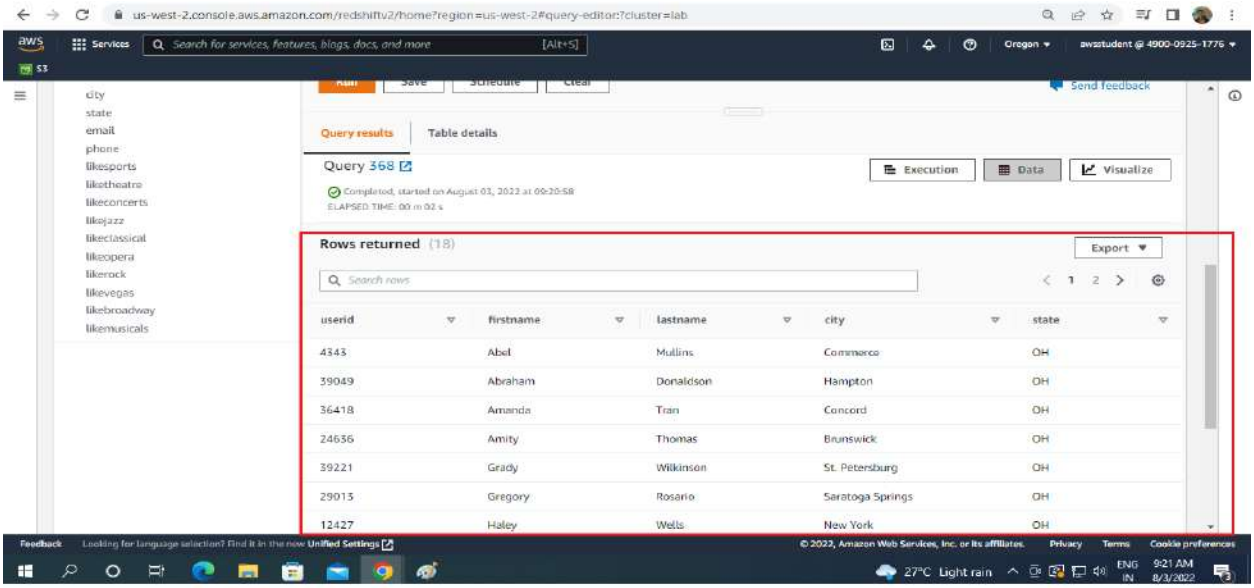
The result shows that there are almost 50,000 rows in the table.

Step 21 – Run this query:

```
SELECT userid, firstname, lastname, city, state FROM users WHERE likesports AND NOT likeopera AND state = 'OH'
ORDER BY firstname;
```

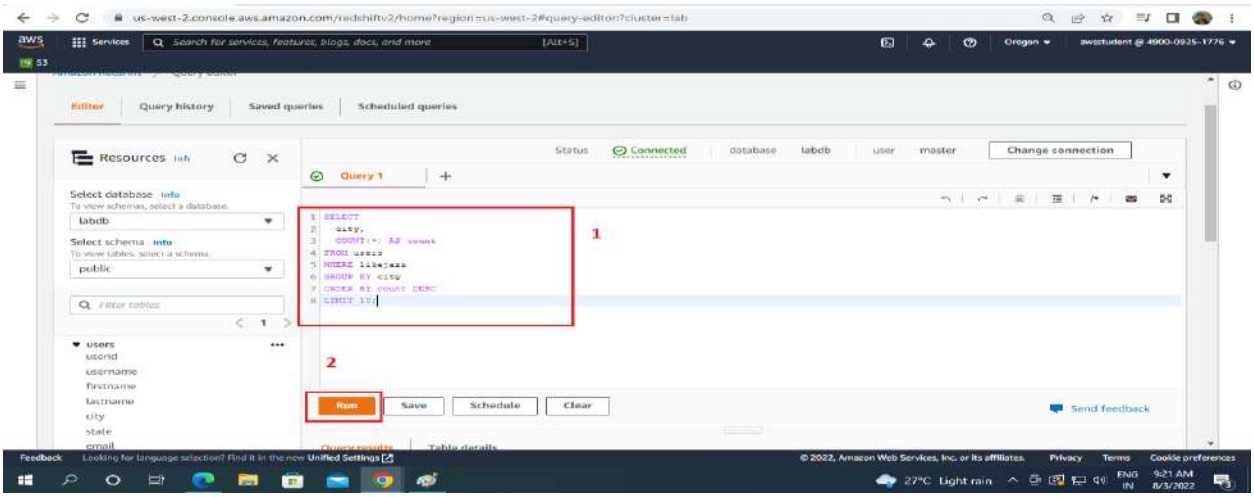


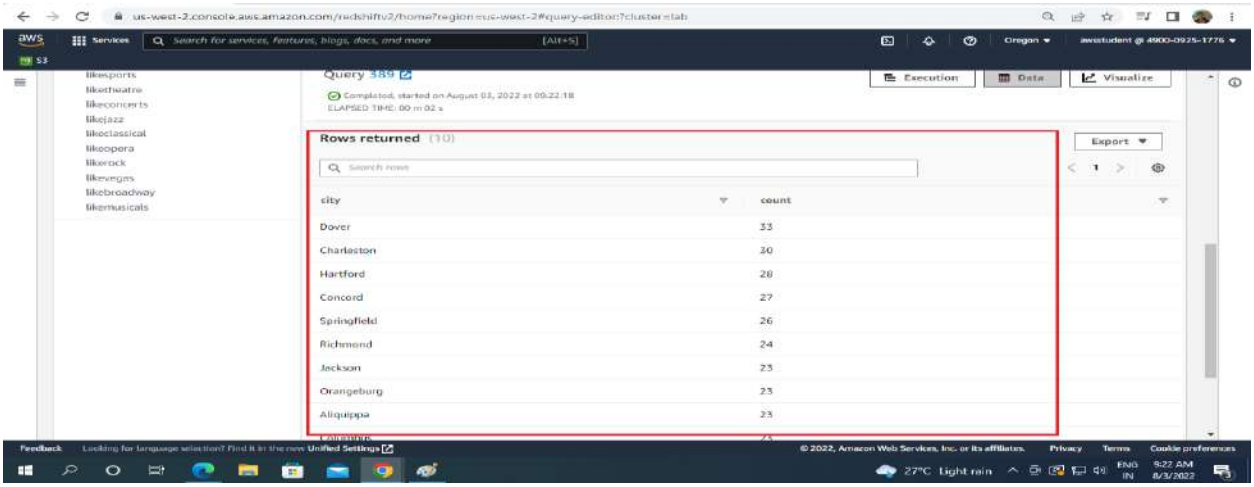
This query displays users in Ohio (OH) who like sports but do not like opera. The list is sorted by their first name.



Step 22 – Run this query:

```
SELECT city, COUNT(*) AS count FROM users WHERE likejazz GROUP BY city ORDER BY count DESC LIMIT 10;
```

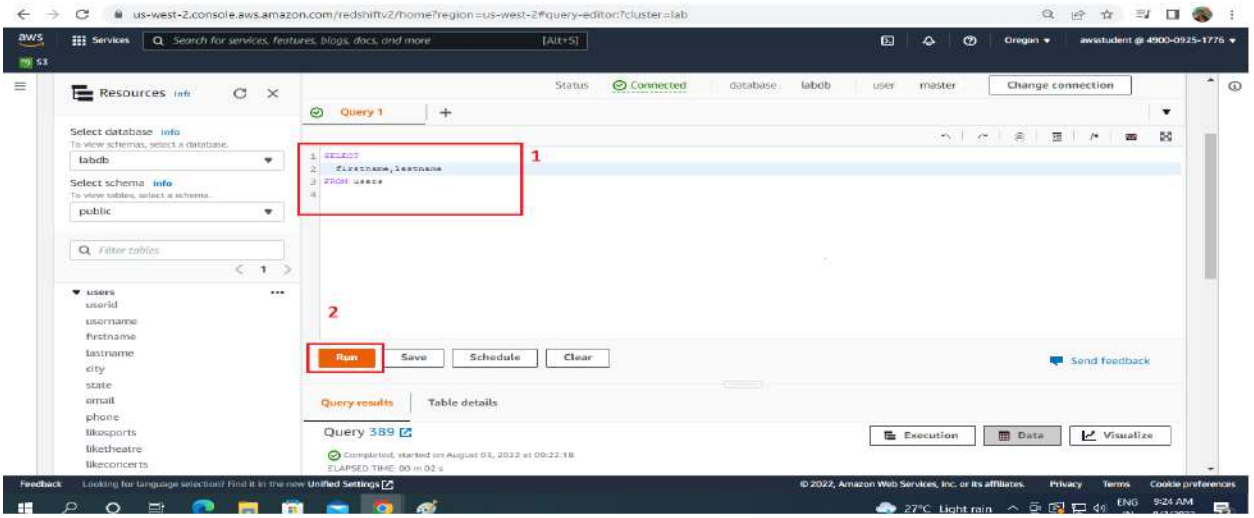


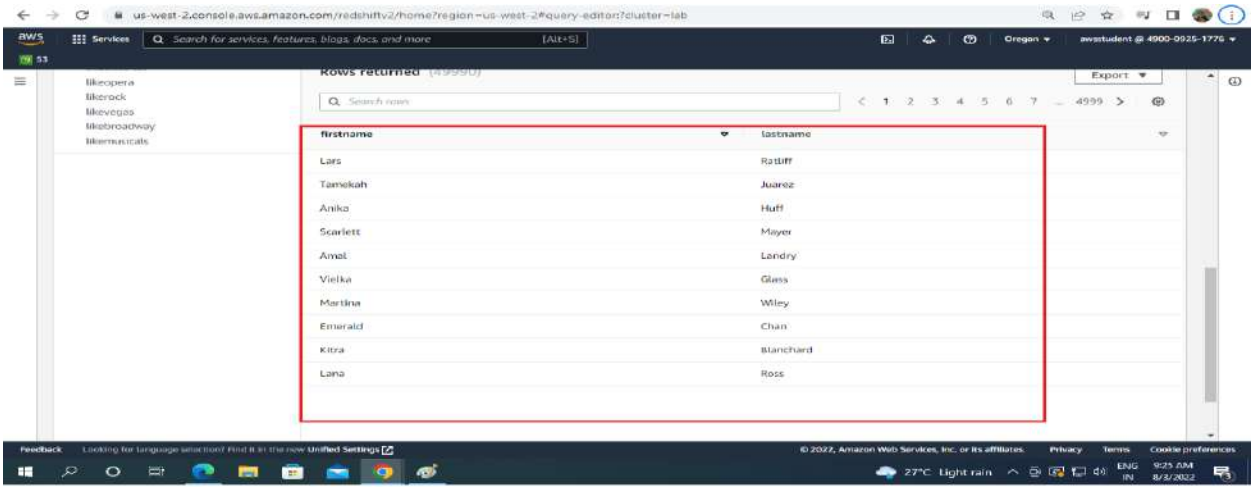


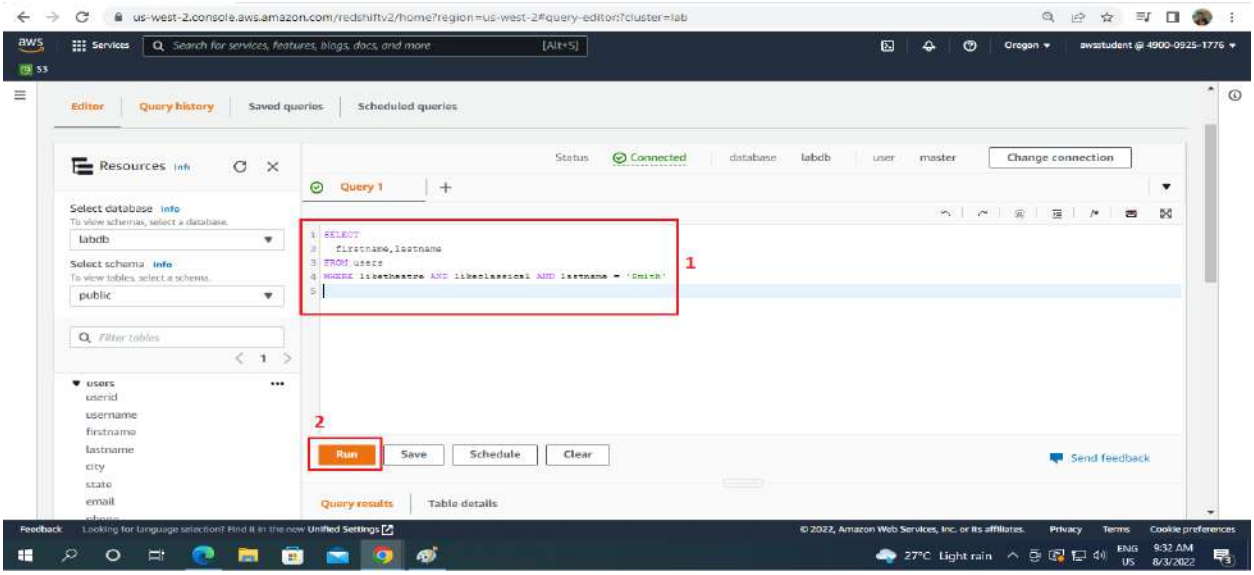
This query shows the Top 10 cities where Jazz-loving users live.

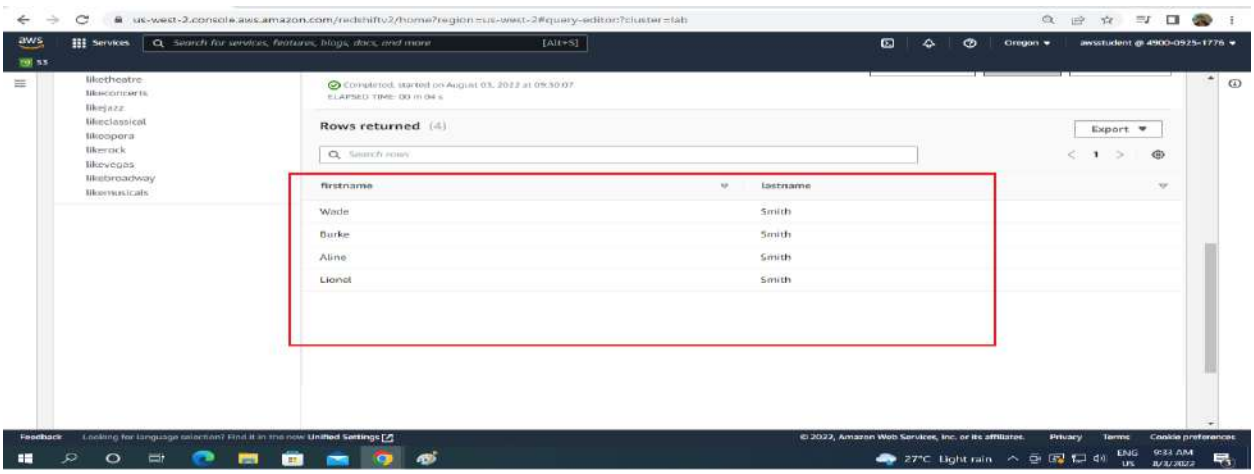
Step 23 – Challenge

- Only display the firstname and lastname
- of users who like both Theatre and Classical music
- With a last name is Smith

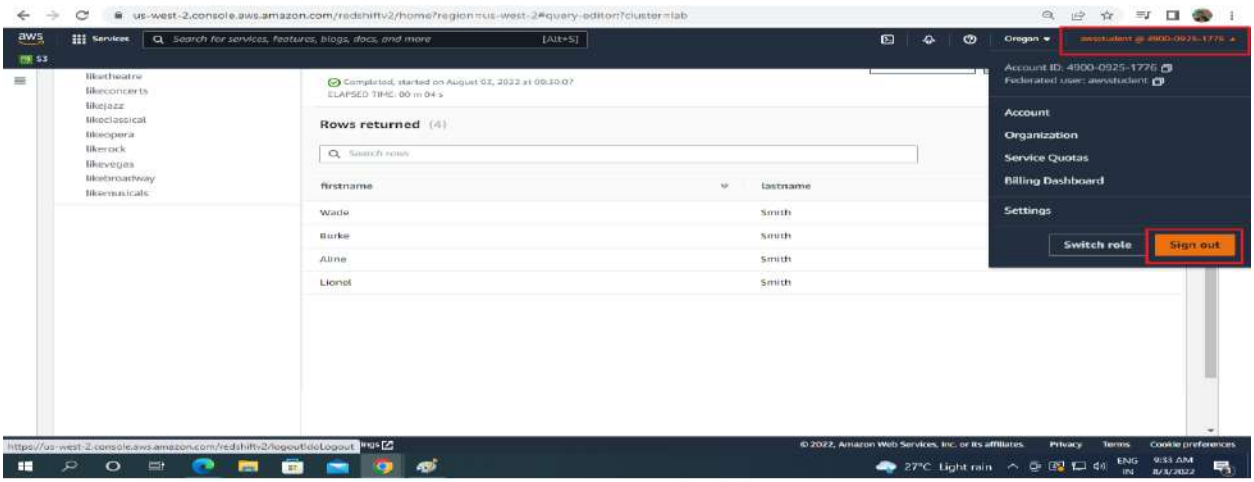

Resources
Select database
labdb
Select schema
public
users
userid
username
firstname
lastname
city
state
email
phone
likesports
liketheatre
likeconcerts
Query 1
SELECT
firstname,lastname
FROM users
1
2
Run
Save
Schedule
Clear
Send feedback
Query results
Table details
Query 389
Execution
Data
Visualize


likeopera
likerock
likevegas
likebroadway
likemusicals
Export
firstname
lastname
Lars
Ratliff
Tamekah
Juarez
Aniko
Huff
Scarlett
Mayer
Amal
Landry
Vielka
Glass
Martina
Wiley
Emerald
Chan
Kitra
Blanchard
Lana
Ross

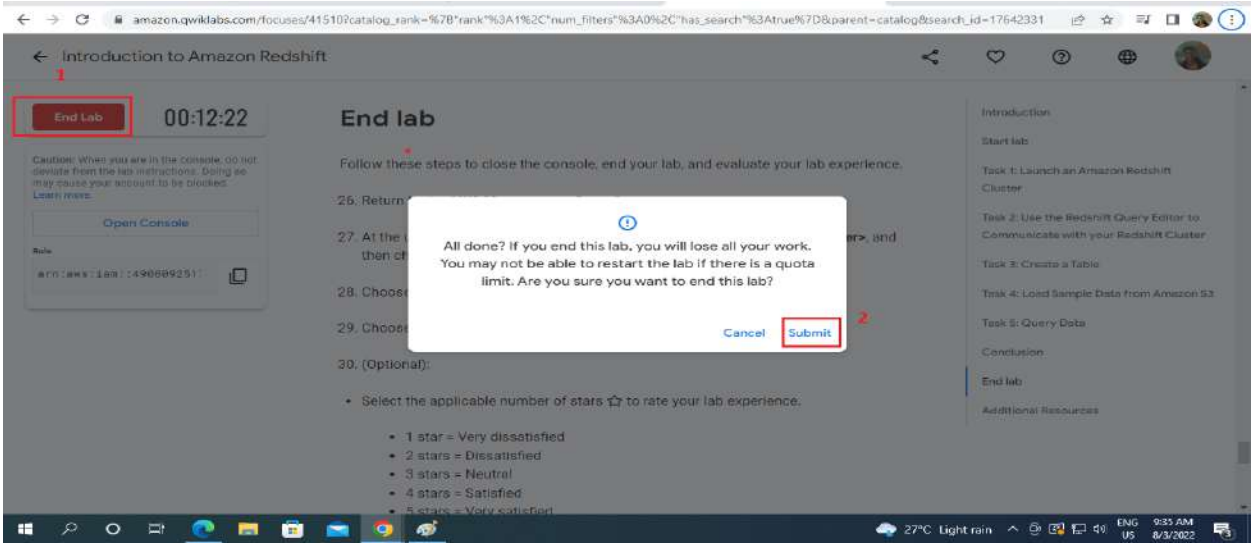

Editor
Query history
Saved queries
Scheduled queries
Resources
Select database
labdb
Select schema
public
users
userid
username
firstname
lastname
city
state
email
Query 1
SELECT
firstname,lastname
FROM users
WHERE liketheatre AND likeclassical AND lastname = 'Smith'
1
2
Run
Save
Schedule
Clear
Send feedback
Query results
Table details



Return to the **AWS Management Console**. At the upper-right corner of the page, choose **awsstudent@<AccountNumber>**, and then choose **Sign out**.



Choose **End Lab** and Click **Submit** button



Practical 7: Introduction to AWS device Farm

A. Create KMS master key Locate or Download an Example Android * .apk and iOS *. ipa File

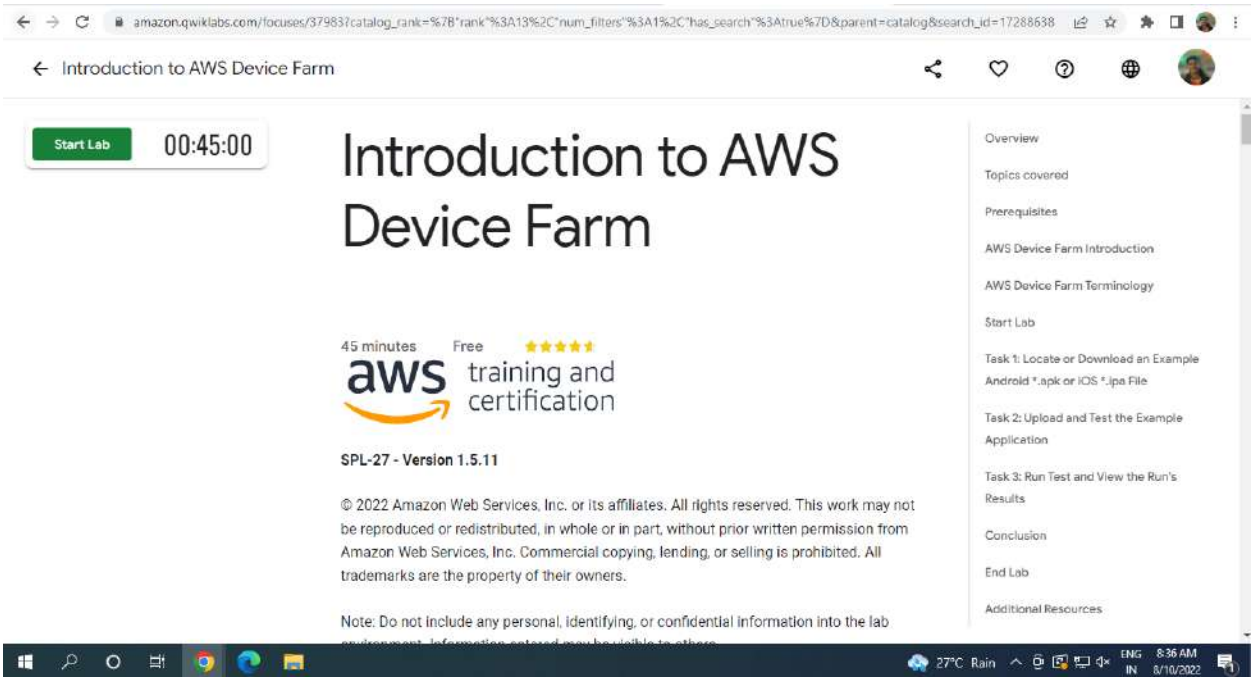
B. Upload and Test the Example Application

C. Run Test and View the Run's Results

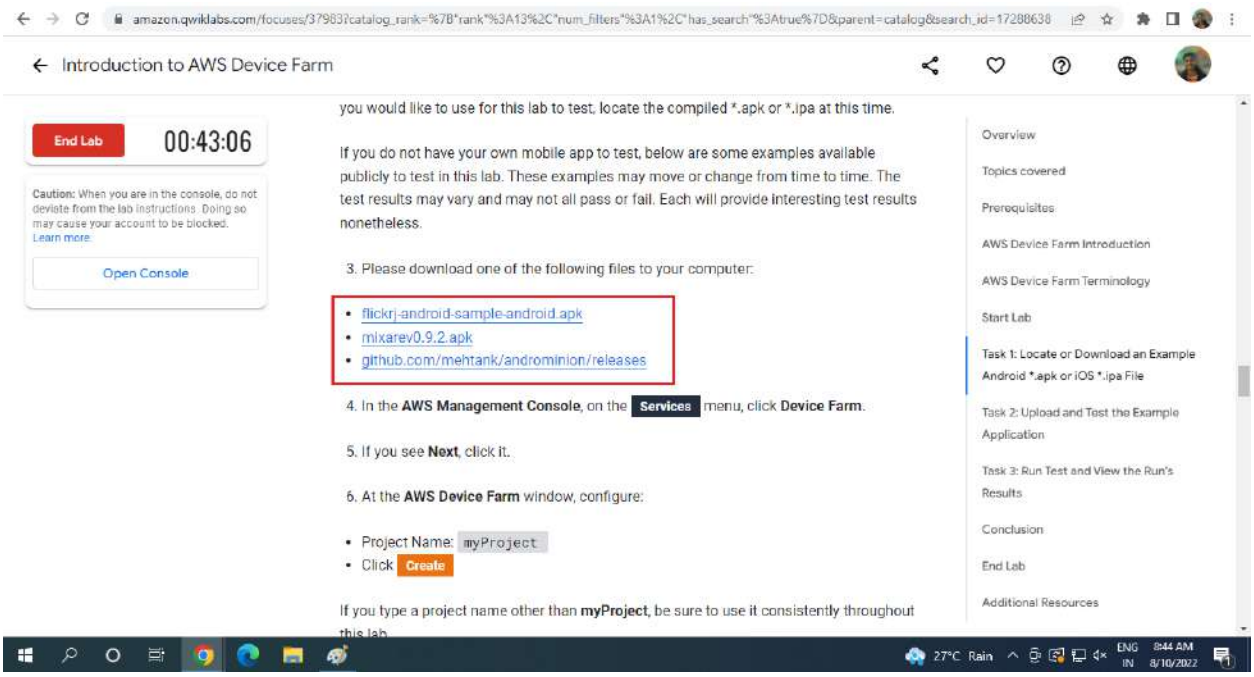
Task 1: Locate or Download an Example Android *.apk or iOS *.ipa File

Step 1 – Go to the given link https://amazon.qwiklabs.com/focuses/37983?catalog_rank=%7B%22rank%22%3A13%2C%22num_filters%22%3A1%2C%22has_search%22%3Atrue%7D&parent=catalog&search_id=17288638

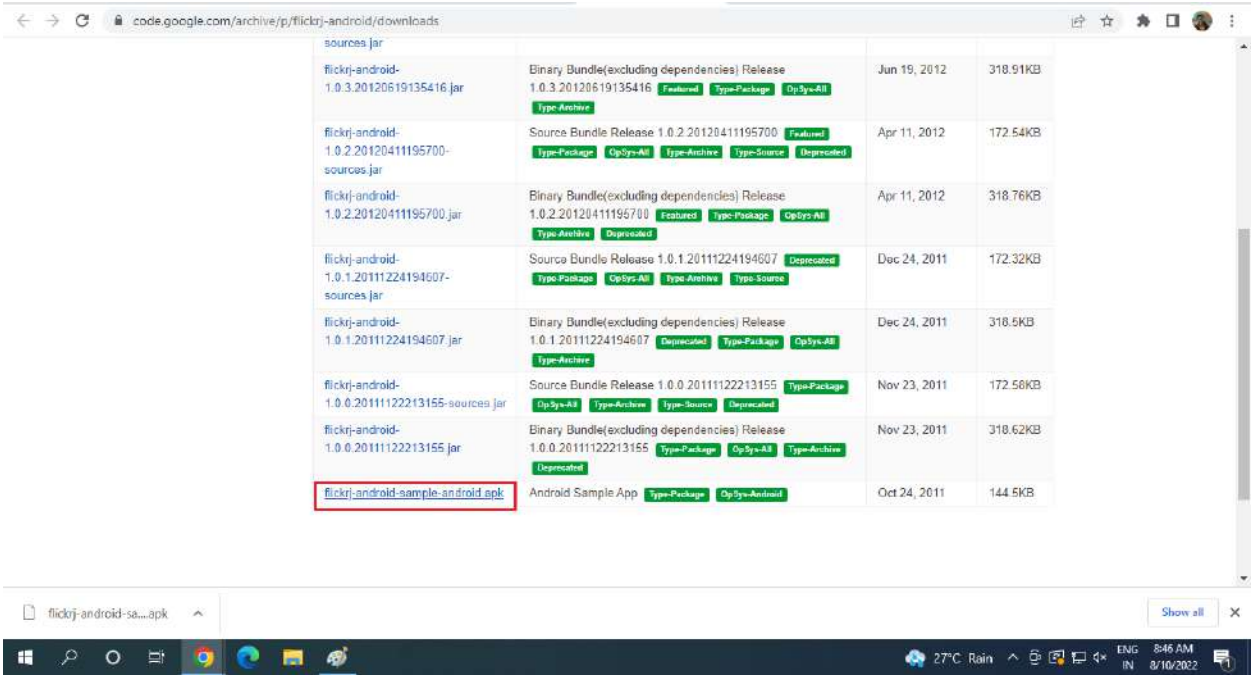
Step 2 – Click on **Start Lab** button.



Step 3 – Download one of the following files.

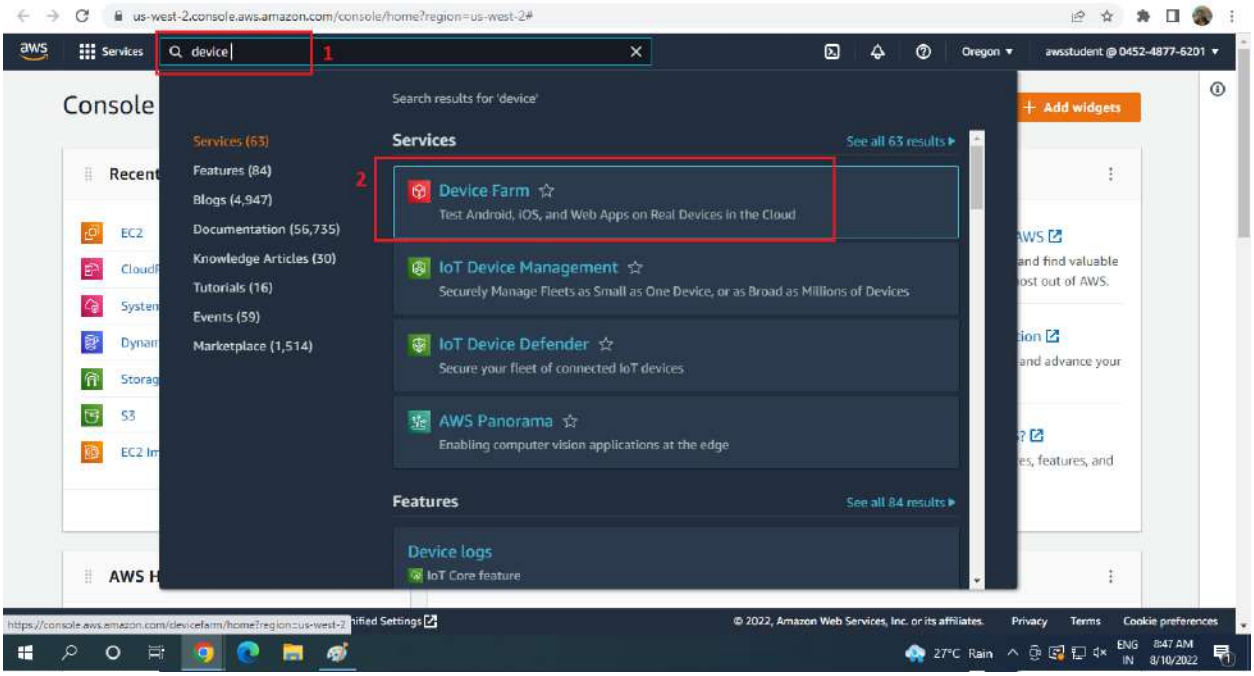


Step 4 – Download the file - flickrj-android-sample-android.apk**.**

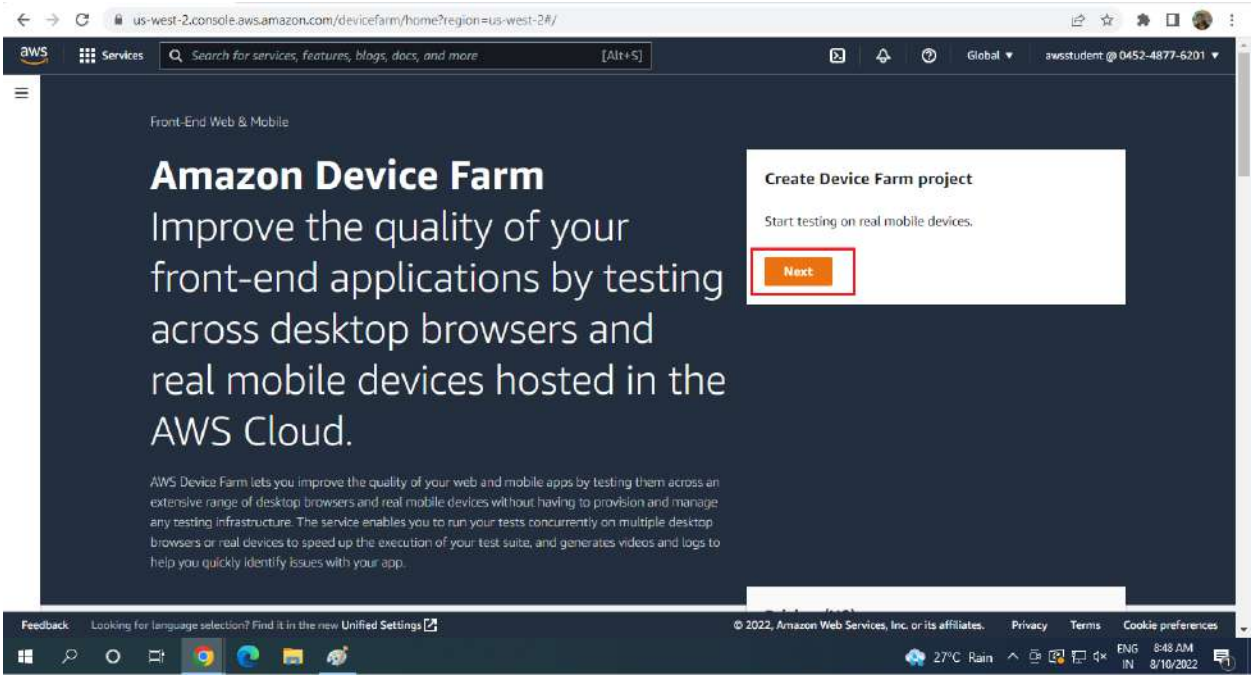


Step 5 – Click on **Open Console** button.

Step 6 – In the Service search bar, search **Device Farm**.

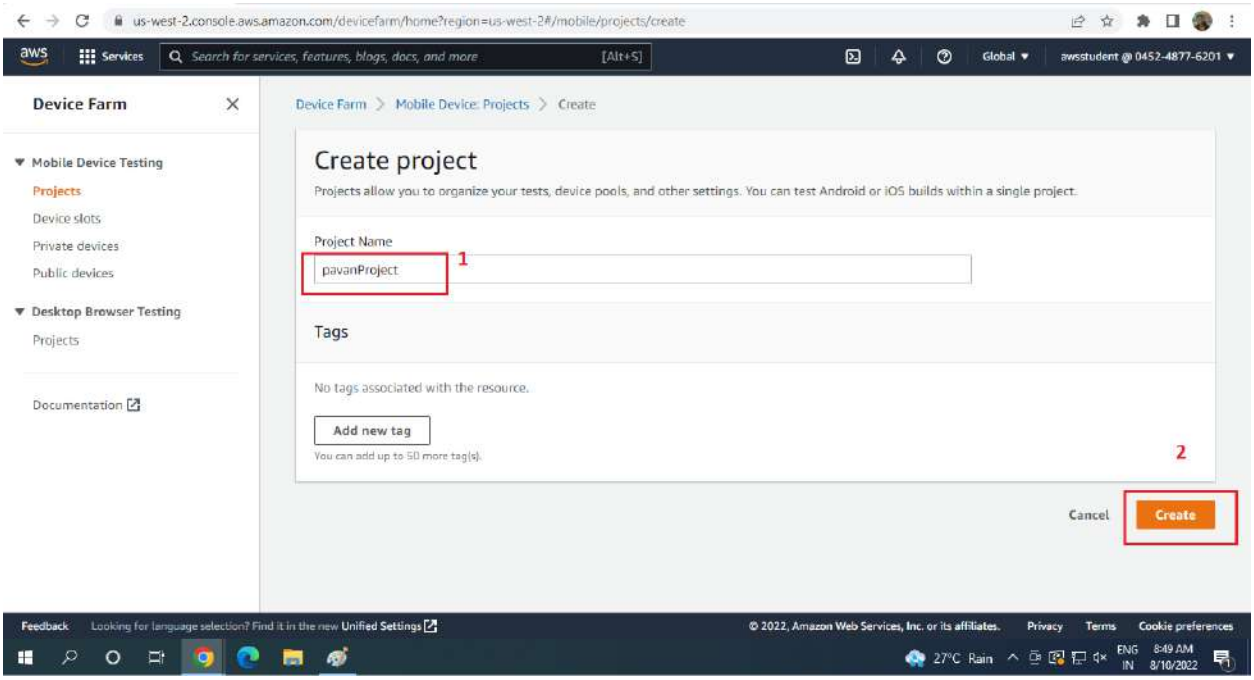


Step 7 – Click on **Next** button.

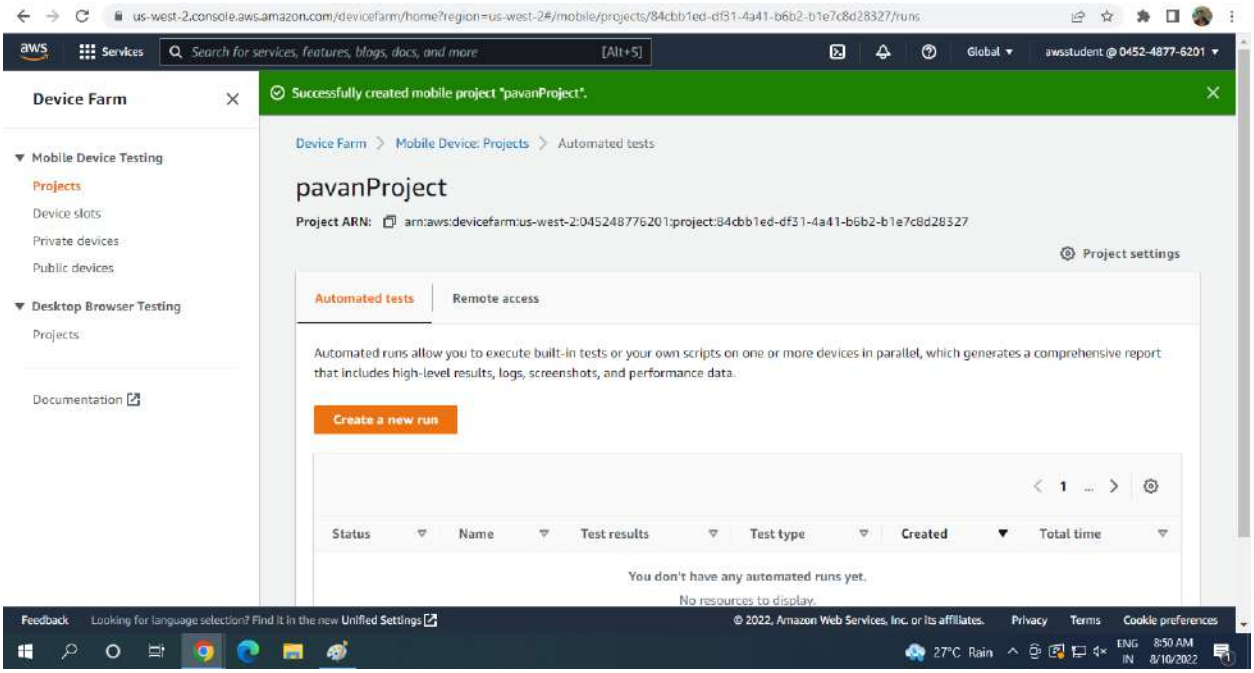


Step 8 – Enter the **Project Name** and then click on **Create**.

Project name: **pavanProject**

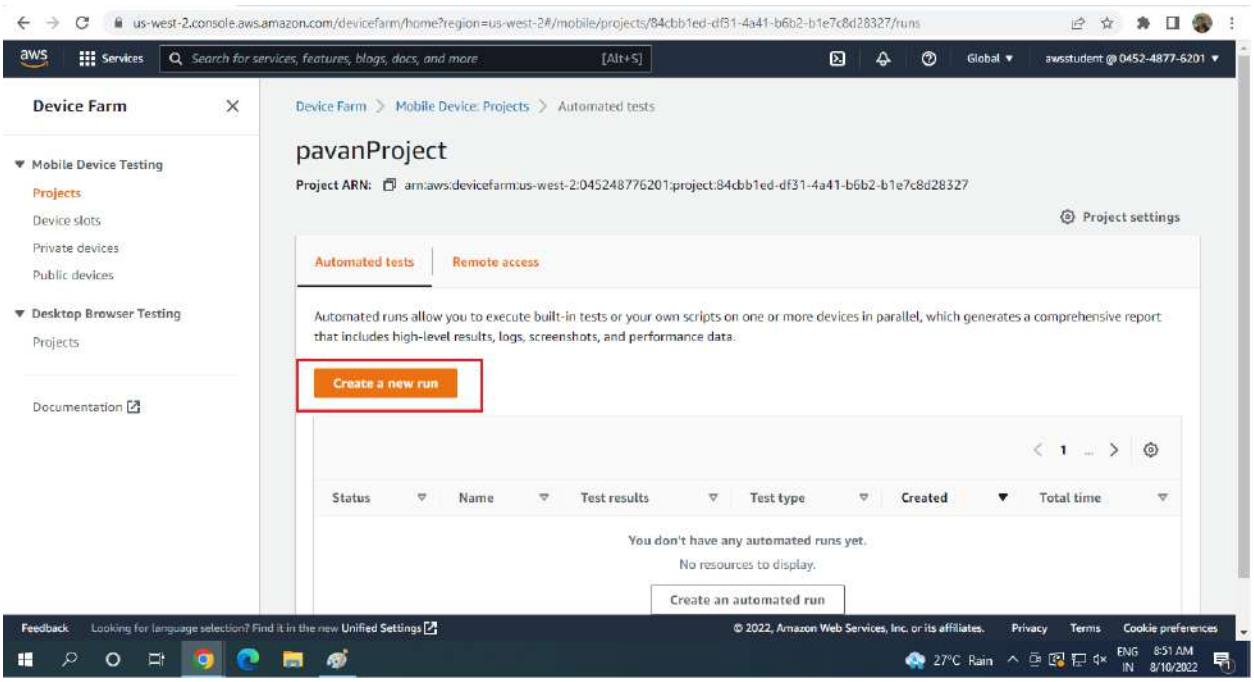


New project is created.



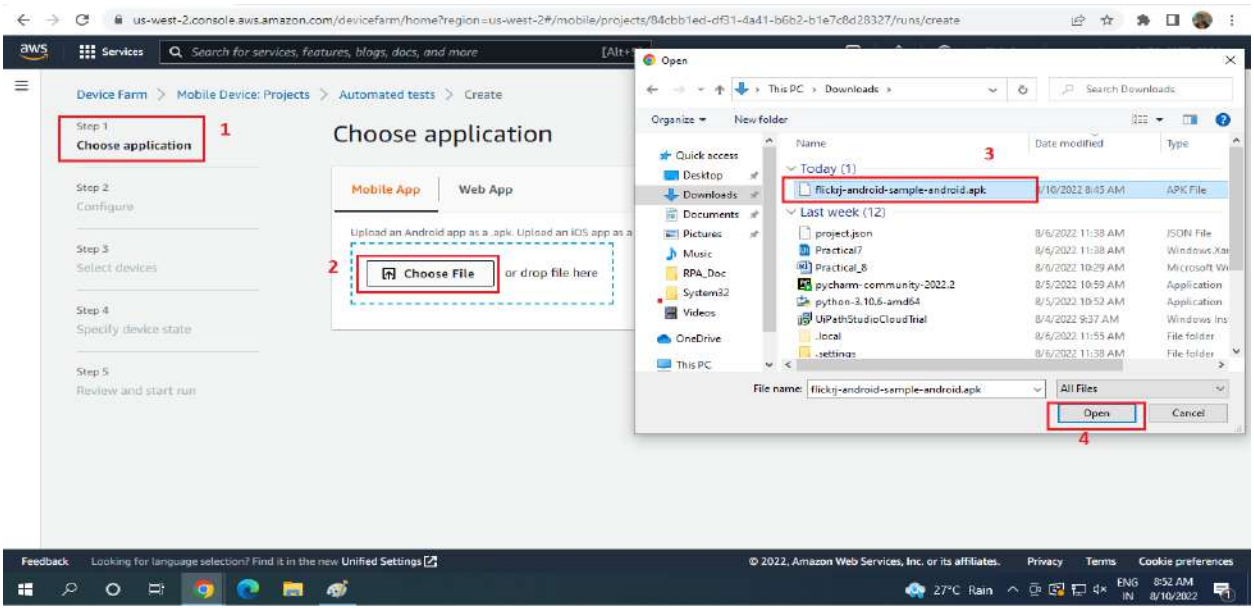
Task 2: Upload and Test the Example Application

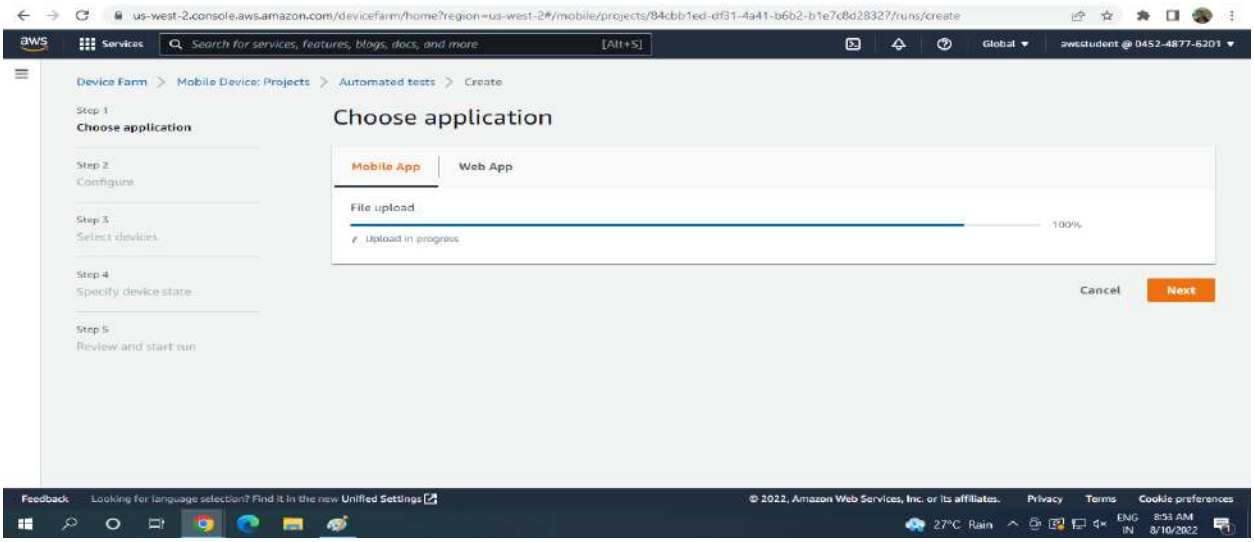
Step 9 – Click **Create a new run**



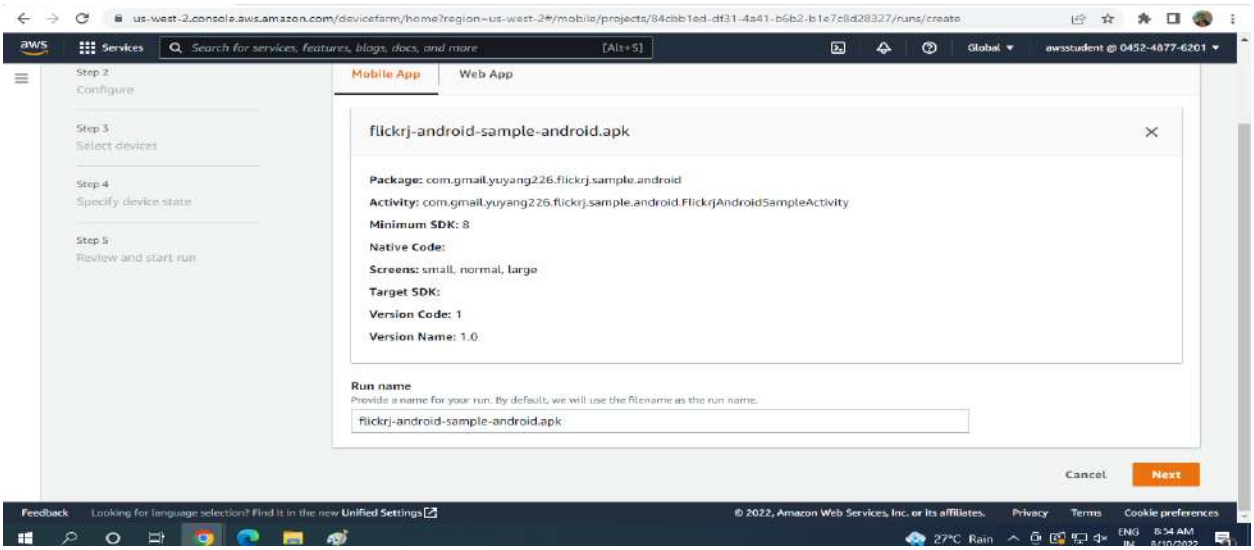
Step 10 – On step 1 - Choose application, configure the following:

- Click Upload.
- Browse to and select the application that you downloaded.

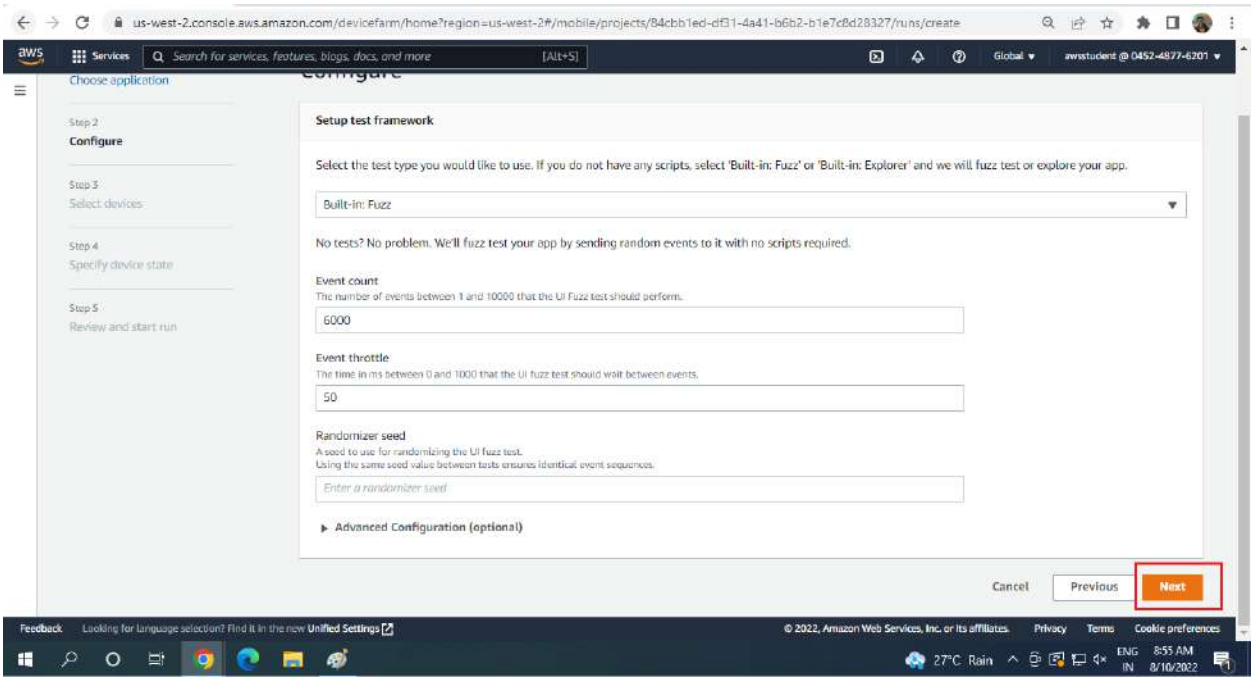




Step 11 – Click **Next**.

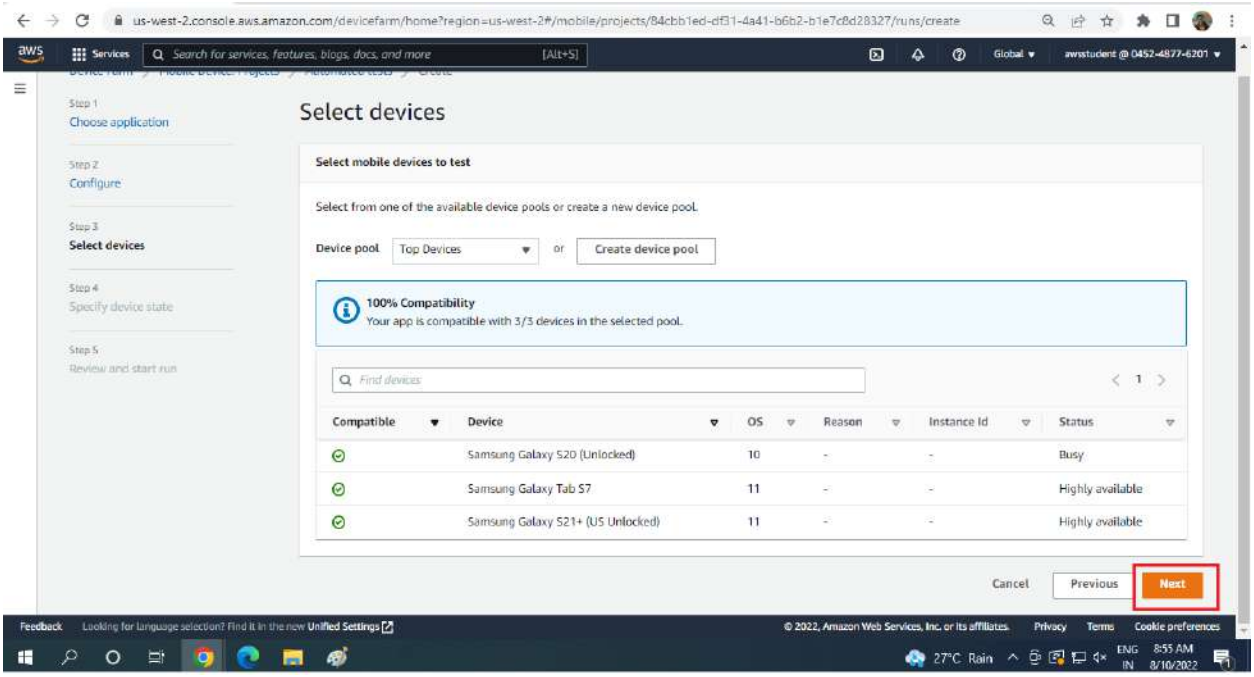


Step 12 – Click **Next**.

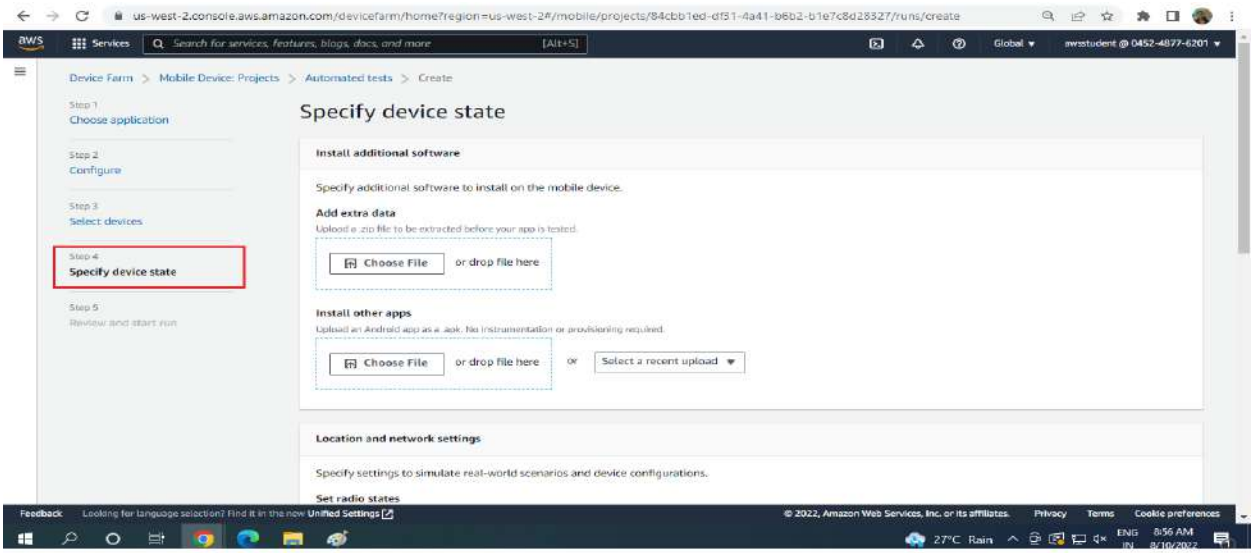


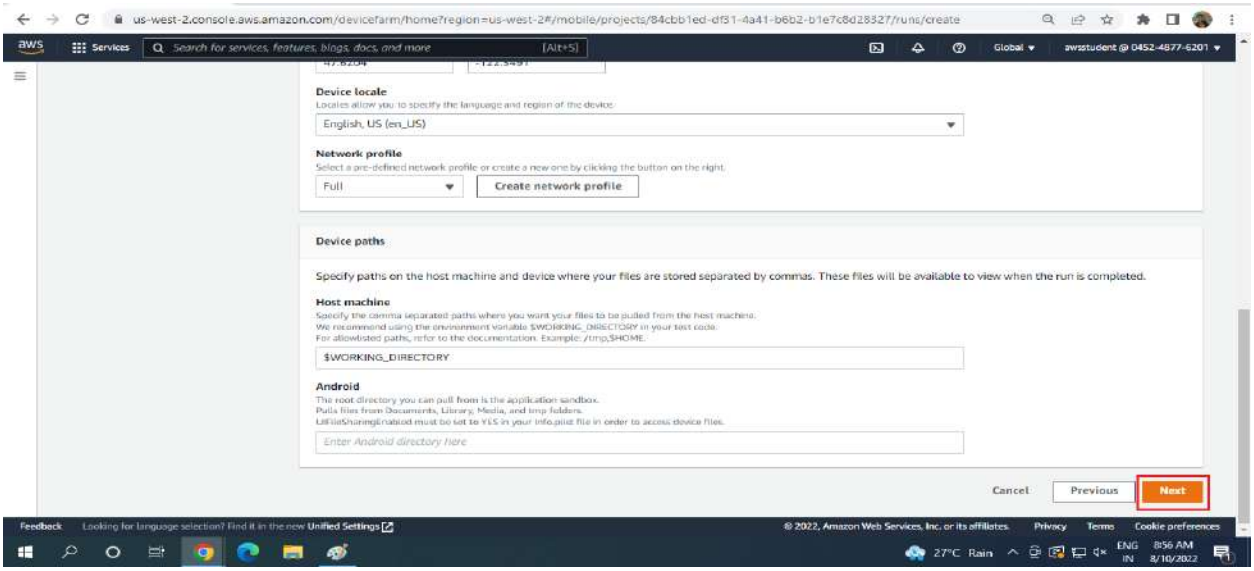
Step 13 – On the **Select devices** page, Click **Next**.

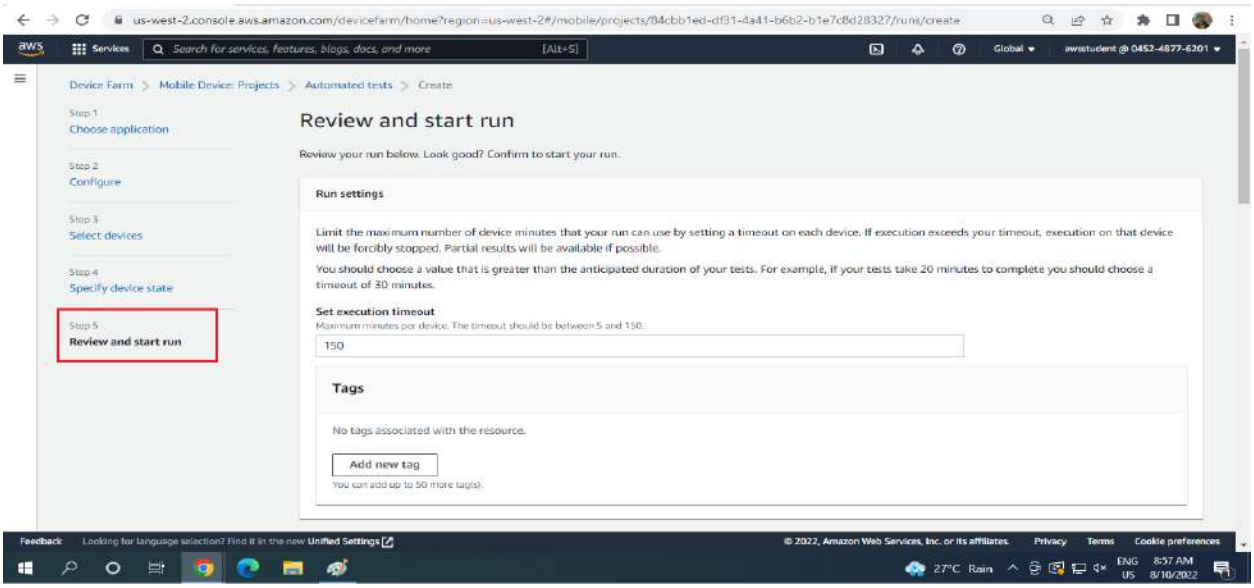
You will see the **Top Devices** pool.



Step 14 – On the **Specify device state** page, Click **Next**.



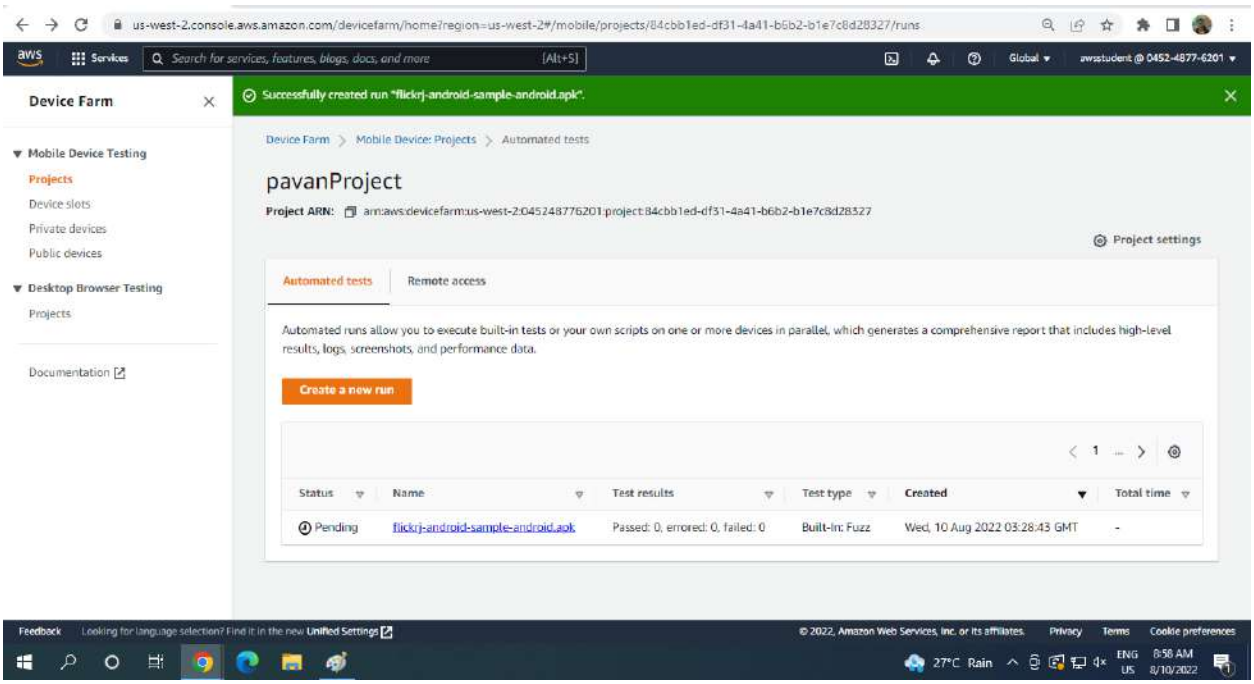


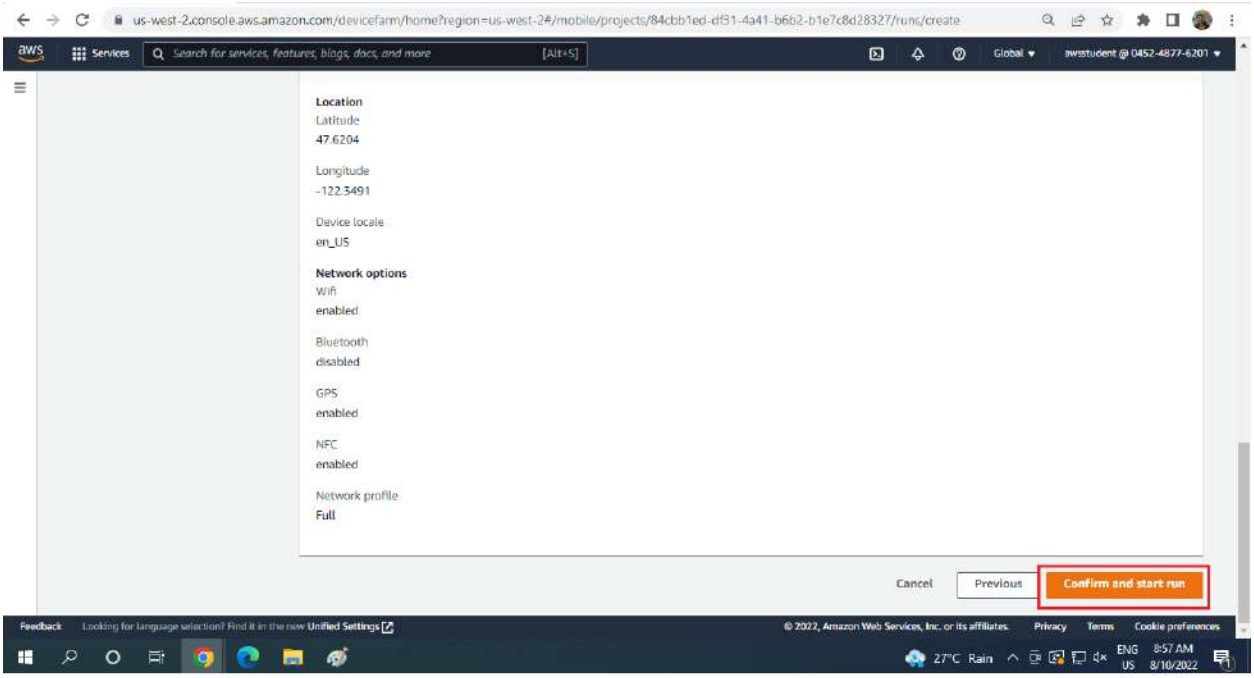


Task 3: Run Test and View the Run's Results.

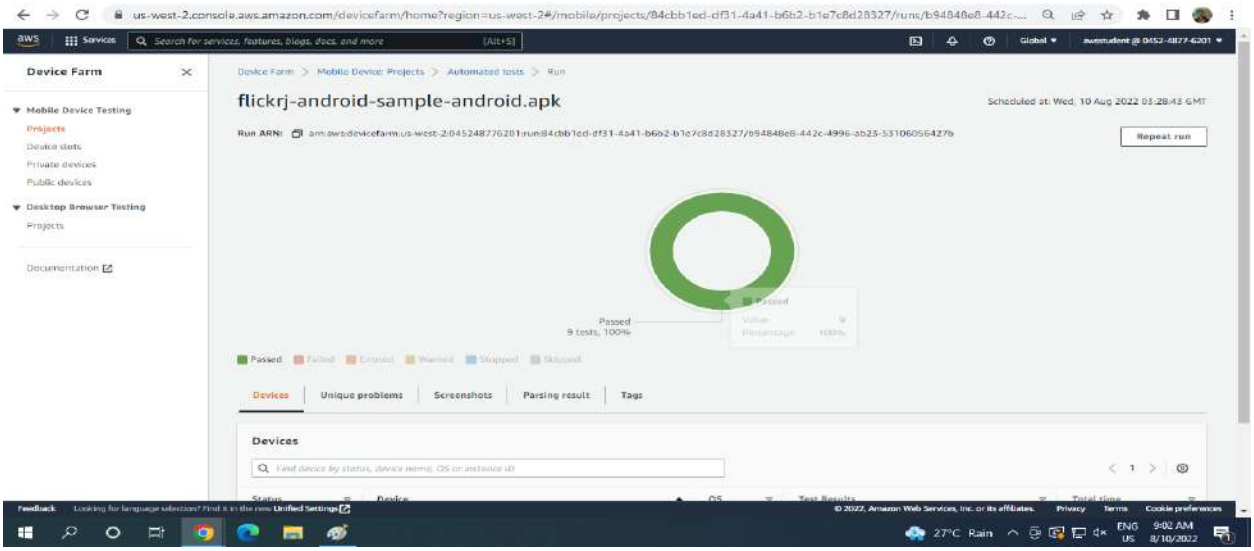
Step 15 – On the **Review and Start Run** page:

- Review your Setting
- Click **Confirm and Start run**



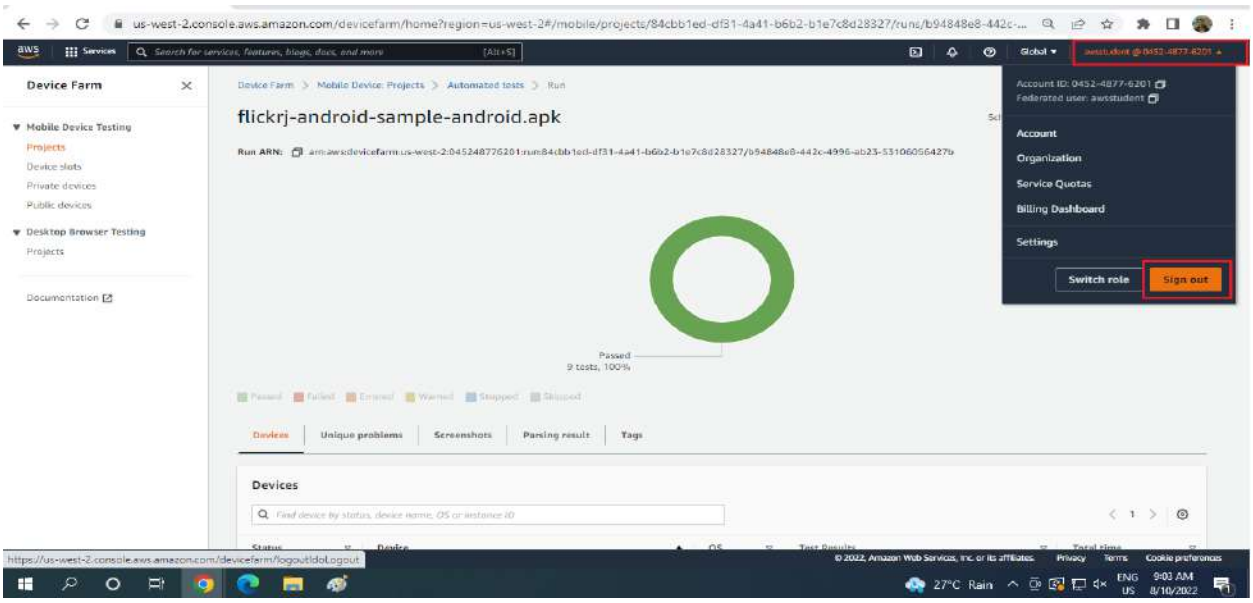


A summary page that includes the following information is displayed.

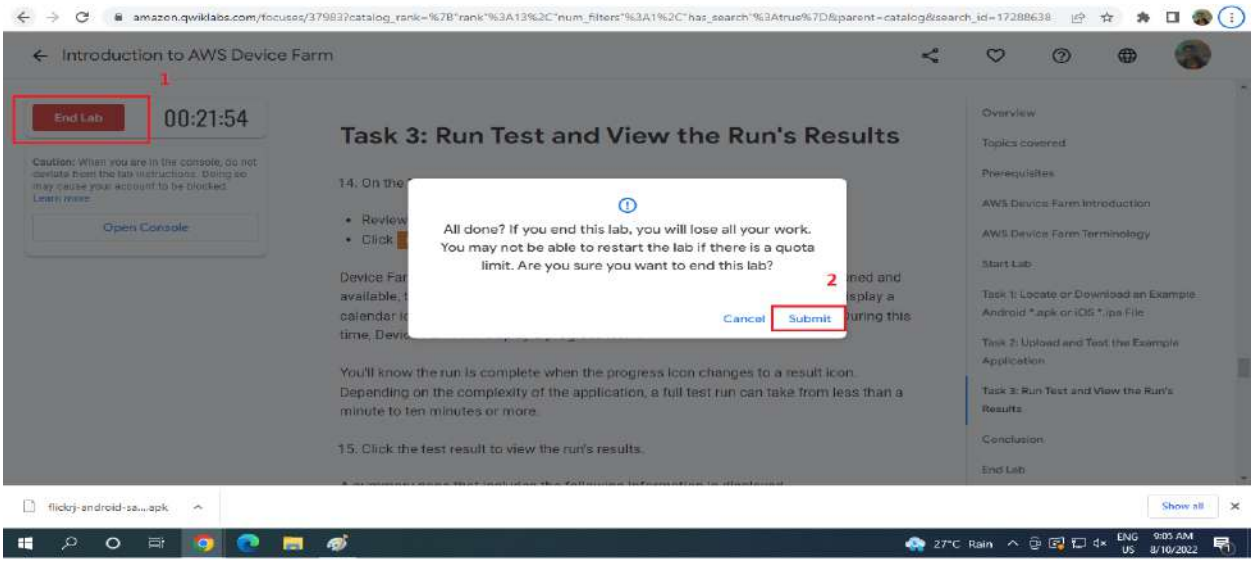


- A list of devices and test results for each
- The total number of suites, by outcome
- Lists of tests with unique warnings or failures
- Screenshots captured during the run, grouped by device

On the navigation bar, choose **awsstudent@<AccountNumber>**, and then choose **Sign Out**.



Choose **End Lab** button, click on the **Submit** button



Practical 8: Case Study's

A. ABP News

B. Buzzdial

C. Classle

D. LIFEPLATE

ABP News

1. Introduction

- ABP News Network (ANN)—one of the largest TV networks in India—operates five news channels in Indian languages such as Hindi, Marathi, Bengali, Punjabi, and Gujarati, and reaches out to more than 150 million TV audiences per week.

2. Before Cloud - Challenges

- News in India can occur in a more dynamic, volatile, and unpredictable way compared to other international markets.
- This means spikes in traffic to digital and mobile news services can occur at any time of the day with minimal warning.
- A major breaking news story can increase traffic by three times, rising to six times for elections that may occur as often as once a year.
- It was therefore extremely important for ANN to scale the technology infrastructure quickly to support these traffic spikes. Furthermore, similarly to international consumers, Indian audiences were increasingly consuming news through digital and mobile services, as well as through broadcast and print. Videos uploaded online were increasingly complementing broadcast and text-based news services.
- In 2013, ANN predicted extending its digital presence from a single website to a range of services could increase its page views from 150 million to over 500 million. The business had to sustain this growth cost-effectively while delivering the responsiveness and reliability that digital consumers demanded. “Considering all the factors in play, we wanted a robust, cost-optimized infrastructure that was reliable and highly scalable,” says Retesh Gondal, head of digital technology at ANN.
- Unfortunately, ANN’ existing managed service provider technology infrastructure could not meet these challenges. The business’s agreement with this provider made scaling its website at short notice to support traffic spikes difficult and expensive. Furthermore, ANN could not gain the visibility to control and optimize its use of infrastructure resources.
- The business also risked ceding competitive advantage to rival media companies by delivering new websites, mobile services, and other products to market in months rather than weeks.
- The limitations of the infrastructure meant editors would be forced to take up to seven minutes to upload a news video several times longer than a media business operating in a highly competitive marketplace could tolerate.
- Ultimately, ANN risked not being able to deliver news quickly to meet viewer demands for immediacy and secure a strong position in the competitive digital news

market in India. Furthermore, the business could not position itself to enter new geographic markets seamlessly and cost-effectively.

3. After Cloud

- ANN brought its web infrastructure back into an on-premises data center as an intermediate step toward moving to a public cloud. To prepare for that move, the company started conducting due diligence on leading public cloud services with Amazon Web Services (AWS).
- This required working with a cloud provider that could scale quickly to support traffic spikes and longer-term growth in traffic to web, mobile, and video news services. In 2014, the company decided to migrate its infrastructure, applications, and services to AWS.
- ANN completed its initial migration to AWS in only four months and has continued to expand the services running in the public cloud architecture to include additional websites, mobile applications, and a video content management system. “We evaluated all the video content management service providers in our market but determined the best option was to develop a system in-house and use workflow, storage, and video file conversion tools provided by AWS,” says Gondal. ANN uses Amazon Simple Storage Service (Amazon S3) to store video files and Amazon Elastic Compute Cloud (Amazon EC2) to run the system used to manage the video content. Amazon Elastic Transcoder converts ANN’ video files from source to different formats for viewing on a range of devices.

4. Benefits

- Cuts video uploading times from seven minutes to less than one minute
- Supported growth from 150 million to 500 million page views
- Scaled to support traffic spikes of up to six times during peak periods
- The company is running its services including websites, mobile apps, and a video content management system on AWS

5. AWS Service Used

1) Amazon S3
2) Amazon EC2
3) Amazon Kinesis
4) Amazon Lambda

Buzzdial

1. Introduction

- Founded in 2013, Buzzdial builds technologies that enable publishers and broadcasters, as well as brands, to supplement television shows with a cross-screen digital experience that can be accessed on viewers' computers, tablets and mobile phones, and integrated with the broadcast.
- For example: Buzzdial delivered a "rate the debate" interface to smartphones, tablets, and computers that enabled viewers to express their sentiment during a United Kingdom leaders' debate on network TV ahead of a general election.

2. Before Cloud

- Buzzdial selected Amazon Web Services (AWS) as a cloud service provider that could meet its needs. "As we explored options during our establishment phase, AWS emerged as a frontrunner to host our services," says Howard.
- "We found it extremely easy to use and massive in scale, which suited our plans to operate in Australia, Europe, the United States and other markets." The fact AWS operated data centers around the world meant Buzzdial could provision infrastructure and deliver services from locations geographically close to broadcast events in a range of countries.
- The business worked closely with AWS solution architects in New Zealand to determine the best architecture for its service.
- "The teams were extremely helpful in validating some of the ideas we had that made it to market.
- They also helped us reject options that simply weren't going to work," says Howard. To boost Buzzdial's confidence, AWS shared stories about successful AWS customers, provided access to businesses that were undertaking similar projects, and demonstrated deep technical knowledge.
- Buzzdial then developed the first stage of its service and created the supporting AWS architecture in four weeks. Initially the business created a monolithic web application that was not optimized for continuous development.
- As Buzzdial learned more about how AWS performed, its engineers opted to break the application up into a series of smaller, interoperating pieces.
- This process has enabled Buzzdial to pursue an agile software development process over the last 18 months, involving regular releases and continuous development.
- Buzzdial's application now runs in Amazon Elastic Compute Cloud (Amazon EC2) instances residing behind Elastic Load Balancing to distribute incoming traffic in such a way as to maximize fault tolerance and minimize latency.
- The application is distributed across discrete application programming interface, web delivery, caching, and database layers. Amazon Route 53 provides domain name services (DNS) that connect viewers with the required resources in AWS, while

Amazon Relational Database Service (Amazon RDS) for MySQL provides a relational database engine to support the service.

- Caching is undertaken at the Amazon EC2 level to prevent the database infrastructure from being overloaded during periods of high demand. Buzzdial develops the application in house on Mac OS X machines and uses an Apache - Subversion - Beanstalk workflow to develop code for testing in the AWS infrastructure. The infrastructure is hosted in the US East (Northern Virginia) region.
- Other services used include Amazon Simple Storage Service (Amazon S3) and Amazon CloudFront which provide a content delivery network for all static web resources including images, scripts, and style sheets. This significantly decreases load on the Amazon EC2 instances.

3. Challenges

- Buzzdial needed to launch onto an infrastructure that could keep costs low during the business's establishment stage, and increase expenditure as more clients started using the service.
- The organization also wanted to pay for infrastructure on demand rather than invest in servers, storage, and networking resources that would remain underutilized except during traffic peaks for an hour or two during high-profile broadcast events.
- The infrastructure had to be highly available and scalable to support traffic during these events.
- In addition, the infrastructure also had to support Buzzdial's plans to operate in several markets, and locate its services in data centers close to prospective clients and viewers to minimize latency that could disrupt the viewers' second screen experience during television programs.

4. After Cloud

- Buzzdial's application now runs in Amazon Elastic Compute Cloud (Amazon EC2) instances residing behind Elastic Load Balancing to distribute incoming traffic in such a way as to maximize fault tolerance and minimize latency.
- The application is distributed across discrete application programming interface, web delivery, caching, and database layers. Amazon Route 53 provides domain name services (DNS) that connect viewers with the required resources in AWS, while Amazon Relational Database Service (Amazon RDS) for MySQL provides a relational database engine to support the service.
- Caching is undertaken at the Amazon EC2 level to prevent the database infrastructure from being overloaded during periods of high demand
- Buzzdial develops the application in house on Mac OS X machines and uses an Apache - Subversion - Beanstalk workflow to develop code for testing in the AWS infrastructure. The infrastructure is hosted in the US East (Northern Virginia) region.

- Other services used include Amazon Simple Storage Service (Amazon S3) and Amazon CloudFront which provide a content delivery network for all static web resources including images, scripts, and style sheets. This significantly decreases load on the Amazon EC2 instances.

5. Benefits

- Cuts video uploading times from seven minutes to less than one minute
- Supported growth from 150 million to 500 million page views
- Scaled to support traffic spikes of up to six times during peak periods
- The company is running its services including websites, mobile apps, and a video content management system on AWS

6. AWS Service Used

1) Amazon S3
2) Amazon EC2
3) Elastic Load Balancing
4) Amazon Route 53

Classle

1. Introduction

- A cloud-based social learning platform that allows students to connect with other students as well as experts and professionals from academic, research institutes and industry.
- The goal of the company's platform is to assist students pursuing higher education learn and develop skills in a manner unencumbered by socio-economic, location and resource barriers.
- a social enterprise, is currently focusing on rural regions of India where students struggle with resource limitations.

2. Before Cloud

- Amazon Web Services (AWS) has been the foundation of Classle's infrastructure since the company's inception. Vaidya Nathan, Founder and CEO-Classle, explains that AWS allowed the company to begin operations six months ahead of schedule and more economically than had been anticipated. Classle is also impressed with the growing list of additional services offered by AWS, which the company has embraced to help further its own expansion.
- Vaidya Nathan says, "The flexibility, reliability, and elasticity were the reasons for the initial decision to use AWS. Over the past two years, other services coming from AWS

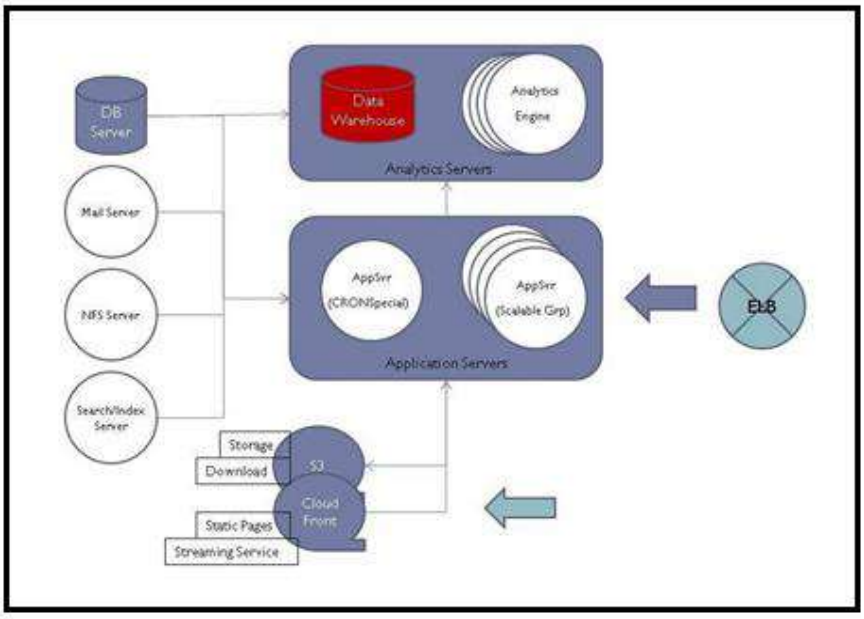
like Amazon Relational Database Service (Amazon RDS), Amazon CloudFront, Amazon CloudWatch, Elastic Load Balancing, and Amazon Route 53 confirm that the decision was the right one. As a startup, we have to worry about balancing scalability with cash preservation, and we get the best of both worlds with AWS. We see AWS as a strategic fit for our long-term business strategy."

- Classle uses Amazon Elastic Compute Cloud (Amazon EC2), with the Amazon Elastic Load Balancing (Amazon ELB), Auto Scaling, and Amazon Elastic Block Storage (Amazon EBS) features, to handle its application and analytics server needs. Amazon RDS acts as Classle's data warehouse and transactional database.
- Amazon Simple Storage Service (Amazon S3), with the Reduced Redundancy Storage (RRS) feature, serves the dual function of providing Classle's content downloads and acting as an origin server for Amazon CloudFront. The company has established Amazon's content delivery service Amazon CloudFront as an edge server for streaming files and delivering the learning platform's most requested video downloads.
- Classle indicates that the origin and edge server relationship the company has created between Amazon S3 and Amazon CloudFront has allowed it to reduce its Webpage load times by 180 percent and reduce its total costs by eight percent and in the case of video streaming, it brought the time-to-market down to 2 days.
- The company monitors its AWS infrastructure with Amazon CloudWatch and uses Amazon Simple Notification Service (Amazon SNS) to delivery system load alerts to its developers. Additionally, Classle routes its users to its websites with Amazon's Domain Name System (DNS) service, Amazon Route.

3. Challenges

- Buzzdial needed to launch onto an infrastructure that could keep costs low during the business's establishment stage, and increase expenditure as more clients started using the service.
- The organization also wanted to pay for infrastructure on demand rather than invest in servers, storage, and networking resources that would remain underutilized except during traffic peaks for an hour or two during high-profile broadcast events.
- The infrastructure had to be highly available and scalable to support traffic during these events.
- In addition, the infrastructure also had to support Buzzdial's plans to operate in several markets, and locate its services in data centers close to prospective clients and viewers to minimize latency that could disrupt the viewers' second screen experience during television programs.

4. After Cloud



5. Benefits

- Based on its success in India, Classle plans to eventually expand its social learning platform to the worldwide market. In the more immediate future, the company is planning a Software-as-a-Service (SaaS) offering of its platform, in addition to the Website-based version.
- As Classle works toward these new goals, it will be looking to incorporate additional services from AWS, such as Amazon Simple Email Service (Amazon SES) and AWS CloudFormation, which assists developers in combining AWS resources within the company's infrastructure.
- Vaidya Nathan says, "Adopting AWS has given our company a competitive advantage, both at tactical as well as strategic levels. Thanks to AWS, we are effectively competing with some large and strong players in the e-learning space. Adopting AWS has let us keep our focus on the business and assume that the infrastructure will be available to match the velocity and growth."

6. AWS Service Used

1) Amazon RDS
2) Amazon CloudFront
3) Amazon CloudWatch
4) Elastic Load Balancing

LIFEPLATE

1. Introduction

- A social-network website that connects people through common interests.
- Members create personalized taglines for use in keyword searches.
- Taglines are used in keyword searches, which enable members to quickly and easily find other people with the same interests, backgrounds, and opinions. Because the website uses a Google map interface, it is easy to connect with other members in the same geographic area.

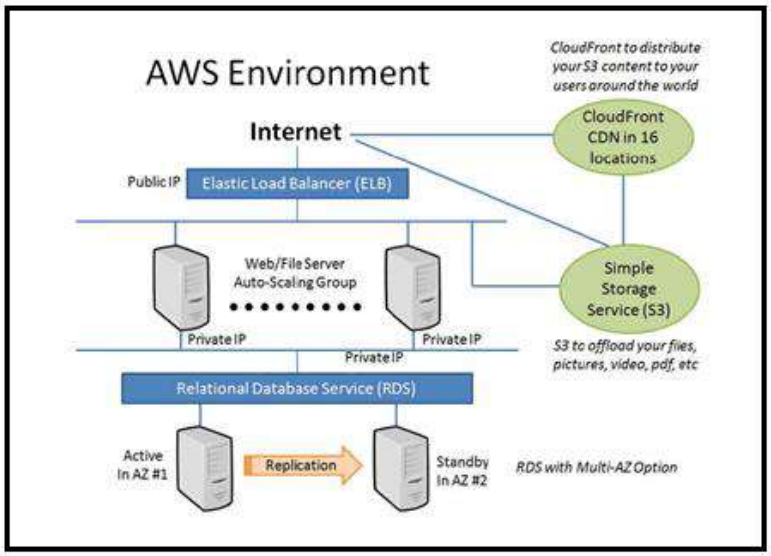
2. Before Cloud

- The website primarily uses PHP, SQL, and JavaScript as its programming languages. Additionally, LIFEPLAT uses available command line tools and PHP libraries to interface with the Amazon API.
- The AWS components of the website are Amazon Simple Storage Service (Amazon S3), Amazon CloudFront, Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing, and Amazon Relational Database Service (Amazon RDS).
- Although LIFEPLAT had some preliminary concerns regarding scalability and server responsiveness, Edward affirms that AWS has been extremely helpful in solving these issues. Amazon S3 and Amazon CloudFront deliver high-speed images to the site's users while providing reliable and unlimited file storage. Because Amazon EC2 scales up or down according to usage, the auto-scaling feature of Amazon EC2 eliminates concerns about the Website handling peak-time operation.
- Elastic Load Balancing automatically distributes incoming application traffic so that processing is more efficient. With Amazon RDS, LIFEPLAT personnel can successfully manage the database in a scalable and responsive way.

3. Challenges

- When deciding to move the website to a cloud platform, LIFEPLAT considered several providers. After a great deal of research, LIFEPLAT determined that Amazon Web Services (AWS) offered the solution which best addressed the company's needs while helping the company solve some key concerns related to scalability and server responsiveness. Edward Hsiao, CEO of LIFEPLAT, explains that "with AWS having an Asia-Pacific presence, it seemed only logical to use AWS, as our current target users are mostly in this area."
- Another deciding factor was the ability to move the website to the cloud without extensive modification to the scripts and database structures. Although security was not initially a key issue for Lifeplat, Edward was extremely pleased to discover that the security measures of AWS were stringent enough to protect the website and its data.

4. After Cloud



5. Benefits

- LIFEPLAT considers its decision to use the AWS solution a wise one.
- Edward explains that the migration process was quite easy and painless, and said “AWS removes my future concerns as a website developer and owner.
- With AWS, I know my website is now able to withstand growth and attacks.”
- The AWS solution is so effective that LIFEPLAT is currently looking into the new features of Amazon RDS.

6. AWS Service Used

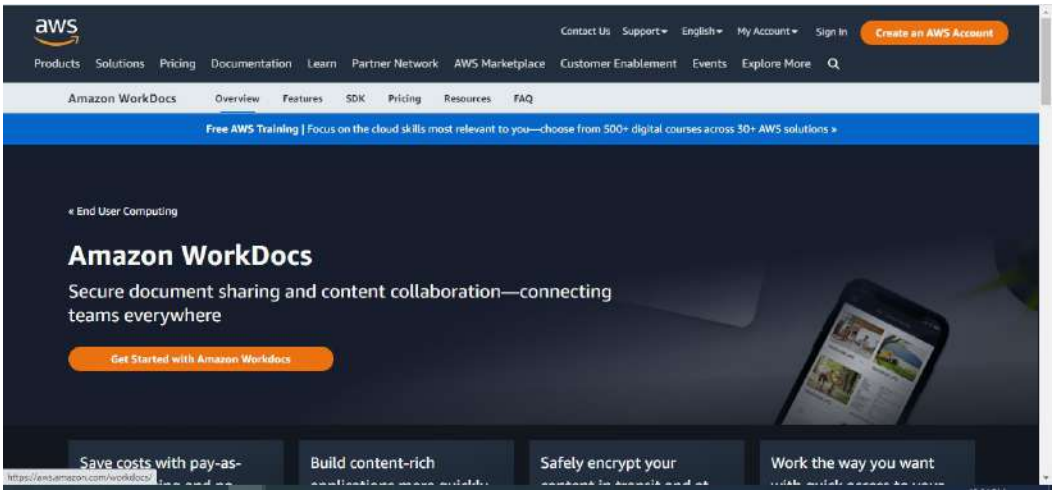
1) Amazon EC2
2) Amazon S3
3) Amazon CloudFront
4) Elastic Load Balancing
5) Amazon RDS

Practical 9: Amazon WorkDocs

- **Amazon WorkDocs** is a fully Amazon managed, highly-secure, enterprise-level storage and sharing service. Unlike $3 based stored files, you can also share your files with other members of your organization for the collaboration or review.
- Before proceeding for the Amazon WorkDocs, let's have a look at what Amazon says about its pricing:
- With Amazon WorkDocs, there are no upfront fees or commitments. You pay only for active user accounts, and the storage you use. In most regions, WorkDocs costs $5 per user per month and includes 1 TB of storage for each user. WorkDocs provides a 30-day free trial with 1 TB of storage per user for up to 50 users. You can invite guest users to log in and view files shared with them at no additional charge."
- As per the above statement, you have 30 days free trial for up to 1 TB of storage that should be more than enough for the learning purpose.

To setup Amazon WorkDocs, you need to perform the following steps:

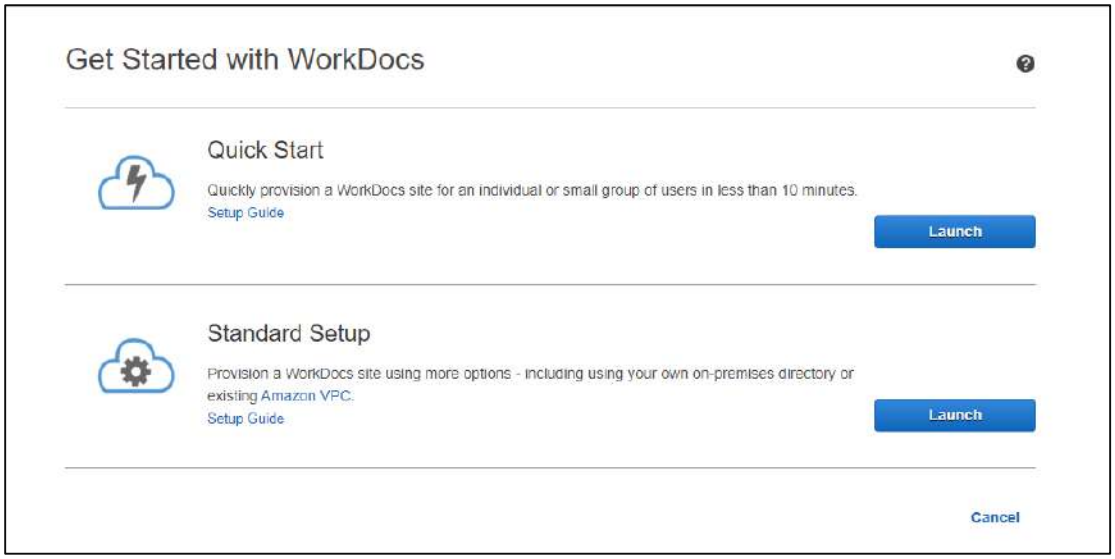
Step 1: Go to the particular link - https://aws.amazon.com/workdocs/



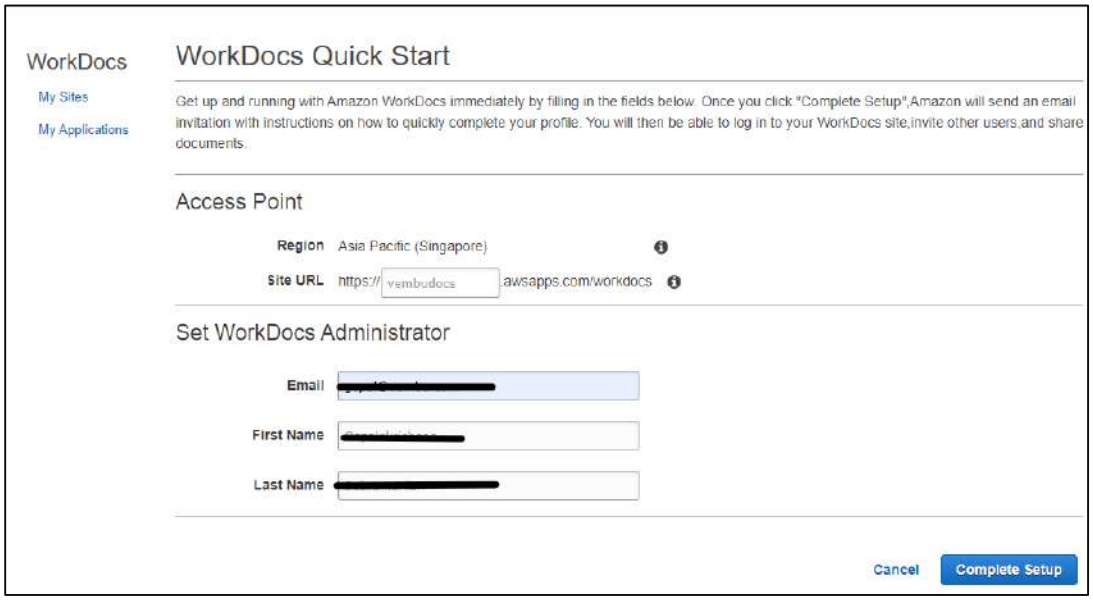
Step 2: Navigate to the Amazon WorkDocs home page for the supported region (not every region supports this feature).

Step 3: Click the Get Started Now button to proceed to the next page.

Step 4: Here, you will see the Quick and Standard setup options as shown in the following figure. For the learning purpose, the Quick Start setup guide should be enough. So proceed with this.



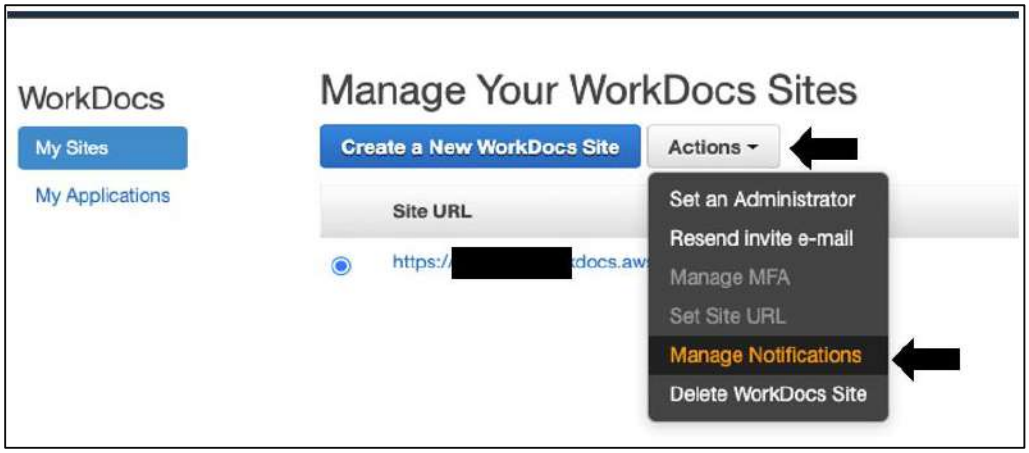
Step 5: On the next page, you need to specify the site URL, email and name details as shown in the following figure.



Step 6: Finally, click Complete Setup to complete the wizard. Your WordDocs site will be started to initialize and should be available after some time. In fact, you will get an email once your WorkDocs site is ready.

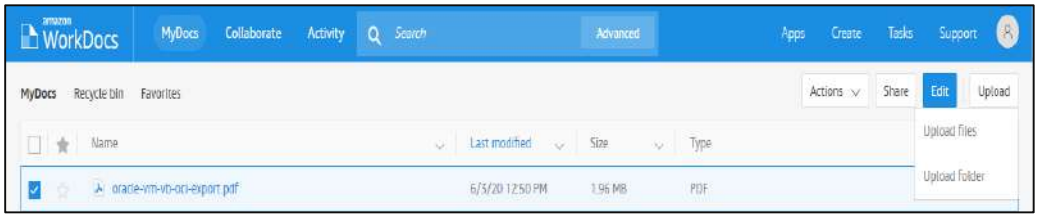
Step 7: Now click the invite link you receive in your email box and set the desired password on the next page.

Step 8: If you didn't get an invite mail yet, select your created WorkDocs site, click Actions, and select Resend invite e-mail as shown in the following figure.

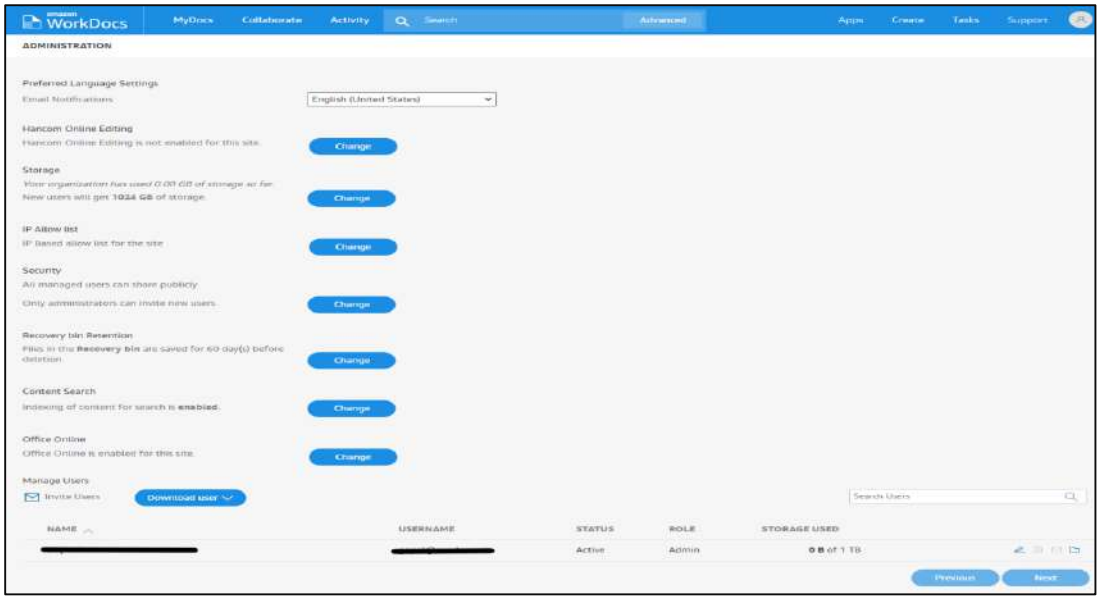


Step 9: Now, click your WorkDocs site link, type your registered email ID and login to WorkDocs console. You will see the WorkDocs console similar to as shown in the following figure.

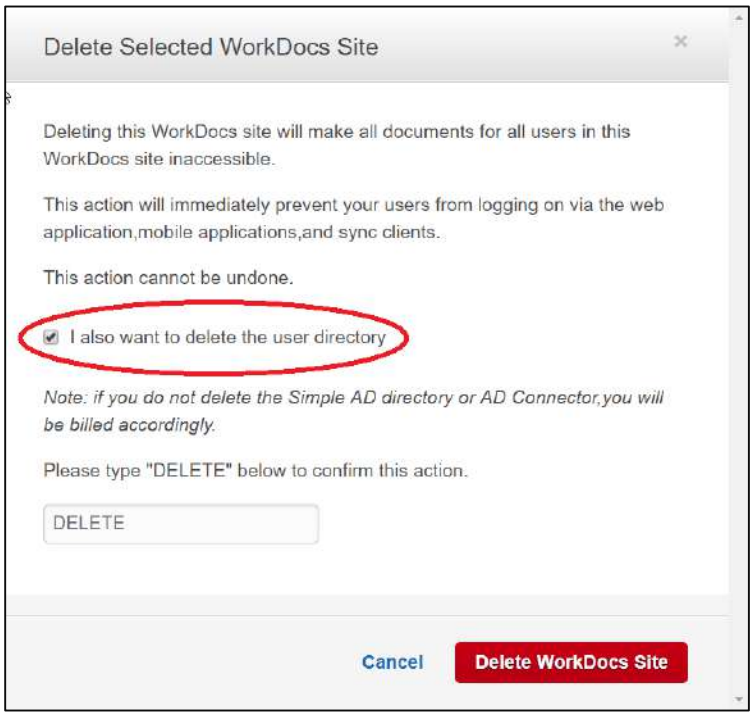
Step 10: In the right pane, you have various options to upload files and folders or create a new folder structure as shown in the following figure.



Step 11: In the left navigation pane, there are various options to work with Amazon WorkDocs as shown in the following figure. We recommend you try to explore each one of them for a few minutes to understand and get familiarized with them.



Step 12: Once your activity is done, please delete your WorkDocs site to avoid any unnecessary charges. For this, select your WorkDocs site, click Actions, and select Delete WorkDocs sites.



Follow the on-screen instructions as shown in the following figure and complete the deletion process.

Practical 10: Managing Virtual Private Cloud

A. Creating VPC in AWS Cloud

B. Creating and Adding Private Subnet in the Existing VPC

C. Deleting VPC

Managing Virtual Private Cloud (VPC)

- VPC is the backbone of the AWS cloud platform. In order to become an AWS Solutions Architect, must have a better understanding of the AWS VPC and Its components.
- if you are from the Networking, background, Managing VPC might be very easy for you, However, candidates from the developing background should spend a good amount of time to get familiarized with the AWS VPC and its Components such as Internet Gateways, NAT Gateways, Routing tables, VPC Peering, Subnets et, we have covered all these components in details in the separate sections, VPC is a separate, isolated, private network in the AWS cloud.
- By default, the instances from one VPC, another VPC cannot communicate to each other, for some reasons, we may need to have multiple VPN in the AWS cloud.
- One use case of having multiple VPCs is that suppose we want to keep our 7 developments and production instances logically isolate to each other.

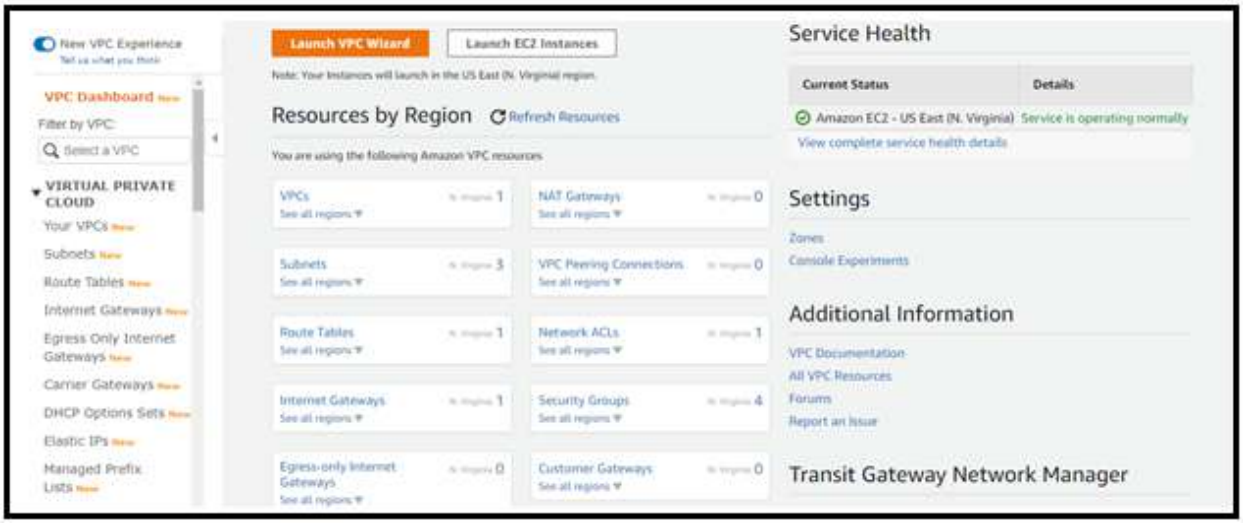
Recommended links:

- Getting started with AWS VPC.
- http://docs.aws.amazon.com/AmazonVPC/latest/GettingStartedGuide/getting-started-ipv4.html)

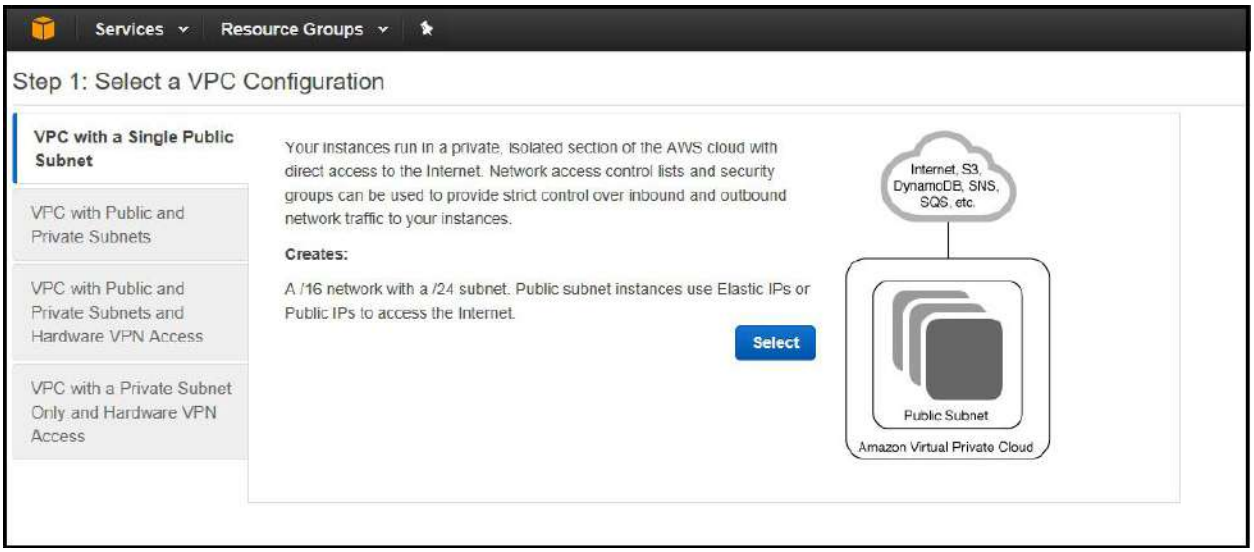
1. Creating VPC in AWS Cloud

In order to create a VPC, you need to perform the following steps:

Step 1: In the AWS console, search and open the VPC dashboard.



Step 2: Click the with Start the VPC Start Wizard option shown in the following figure.



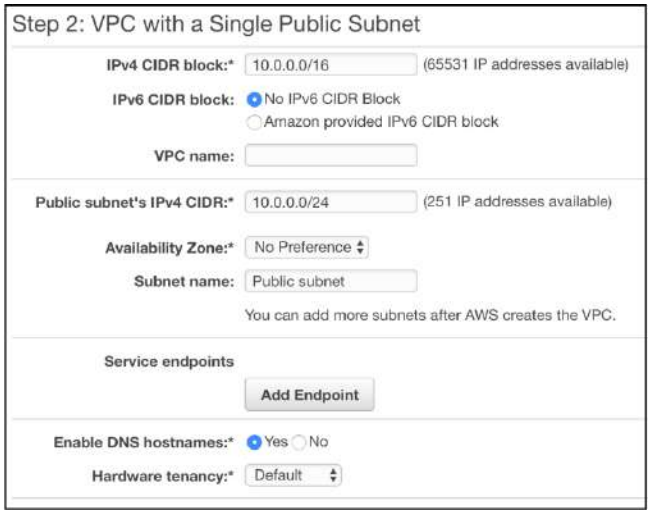
Step 3: On the Select a VPN Configuration page, click each of the VPC Configuration options and review the description of the features provided by them.

Step 4: Depending on your requirement, select the appropriate VPC configuration. Here, we will select the VPC with a Public Subnet option as shown in the following figure.

Step 5: On the next page, specify the VPC name, subnet range, and Availability zone etc. Here we are going to specify the following values:

- **IPv4 CIDR Block:** 10,50.0.0/16
- **VPC Name:** My_Test_VPC

- **Public Subnet CIDR:** 10.50.1.0/24
- **Availability Zone:** Select the first availability zone.
- **Subnet Name:** Public_Subnet1



Step 6: Click the Create VPC button to proceed next. The VPC will be created and available in the VPC list as shown in the following figure.

2. Creating and Adding Private Subnet in the Existing VPC

- Once we had selected the VPC with a public subnet option, so need to create a private subnet separately. A private subnet does not have direct access from the outside AWS network such as the internet.
- All Private subnet require a NAT gateway to access the internet. Typically backed and database servers should always belong to the private subnets.
- If you are interested, you can visit the following link to know more about the AWS VPC and subnets.
- AWS VPC and subnets Getting Started.
- Http://docs.aws.amazon.com/amazonVPC/latest/UserGuide/VPC_Subnets.html

To create a private subnet, you need to perform the following steps

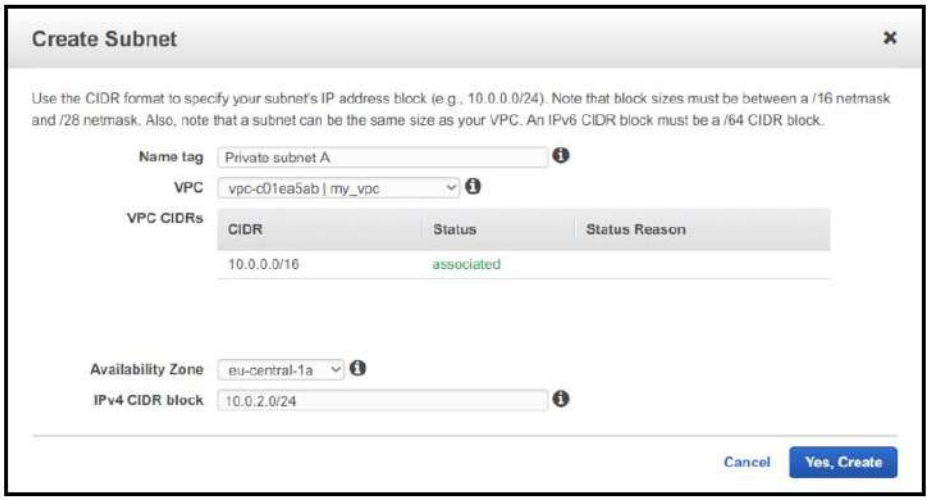
Step 1: Select the Subnets option in the navigation pane and then click Create Subnet.

Step 2: On the Create Subnet page, specify the following values:

- **Name tag:** Name of the subnet
- **VPC:** Select the VPC in which you want to create the subnet
- **Availability Zone:** Select the zone in which you want to create the subnet
- **IPv4 CIDR block:** Specify the subnet IP range which must be within the VPC CIDR range.

Step 3: For our lab exercise, let's create a Private subnet with the following values:

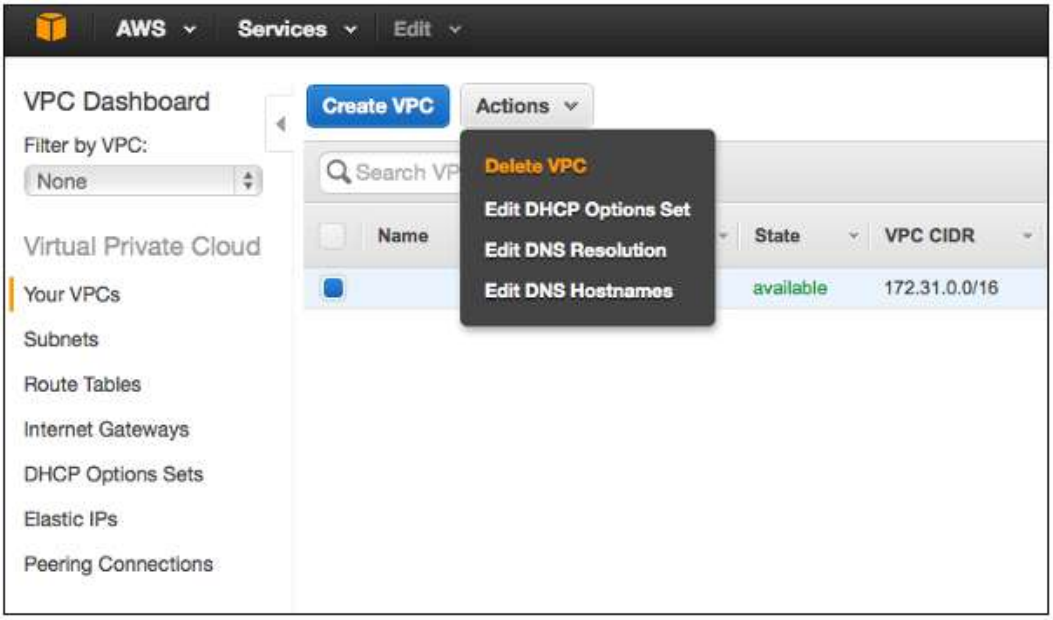
- **Name tag:** Private_Subnet1
- **VPC:** My_Test_VPC
- **Availability Zone:** ap-southeast-2b
- **Iv4 CIDR block:** 10.50.2.0/24



Step 4: Click the Yes Create button to proceed. A new private subnet will be added to your existing VPC.

3. Deleting VPC

If you no longer require any VPC for any reason, you can delete it anytime. For this, just select the VPC you want to delete, click Actions and then select Delete VPC to delete it as shown in the following figure.


AWS
Services
Edit
VPC Dashboard
Filter by VPC:
None
Virtual Private Cloud
Your VPCs
Subnets
Route Tables
Internet Gateways
DHCP Options Sets
Elastic IPs
Peering Connections
Create VPC
Actions
Delete VPC
Edit DHCP Options Set
Edit DNS Resolution
Edit DNS Hostnames
Search VP
Name
State
VPC CIDR
available
172.31.0.0/16