



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: Kedar Sitaram Jadhav

Roll No.: 621

# INDEX

Practical No.	Title	Date	Page No
1	<b>Introduction: Getting Familiarized with AWS Console.</b> <ul style="list-style-type: none"> <li>A. Creating Aws Free Tier Account</li> <li>B. Getting Familiarized with The Aws Console</li> </ul>	15/06/2022	4-18
2	<b>An Aws Iam User: Creating an AWS IAM User.</b> <ul style="list-style-type: none"> <li>A. Explore users and groups.</li> <li>B. Add users to groups</li> <li>C. Sign-In and test the users</li> </ul>	24/06/2022	19-64
3	<b>Working With S3 Buckets</b> <ul style="list-style-type: none"> <li>A. Create a bucket.</li> <li>B. Upload an object to the bucket.</li> <li>C. Make an object public</li> <li>D. Create a bucket policy</li> <li>E. Explore versioning</li> </ul>	29/06/2022	65-89
4	<b>Introduction to AWS Key management Service</b> <ul style="list-style-type: none"> <li>A. Create KMS master key.</li> <li>B. Configure CloudTrail to store Logs in an S3 Bucket.</li> <li>C. Upload an Image to S3 bucket and encrypt it</li> <li>D. Access the encrypted image</li> <li>E. Monitor KMS activity Using CloudTrail Logs</li> <li>F. Manage encryption keys</li> </ul>	05/07/2022	90-120
5	<b>Introduction to Amazon DynamoDB</b> <ul style="list-style-type: none"> <li>A. Create a new table</li> <li>B. Add data</li> <li>C. Modify existing items</li> <li>D. Query the table</li> <li>E. Delete the table</li> </ul>	13/07/2022	121-143
6	<b>Introduction to Amazon Redshift</b> <ul style="list-style-type: none"> <li>A. Launch an amazon redshift cluster.</li> <li>B. Launch Pgweb to communicate with the redshift cluster</li> <li>C. Create a table</li> <li>D. Load sample data from amazon S3</li> <li>E. Query data</li> </ul>	03/08/2022	144-163

7	<b>Introduction to AWS Device Farm</b>  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	164-174
8	<b>Case Study's</b>  A. ABP News B. Buzzdial C. Classle D. LIFEPLATE	17/08/2022	175-185
9	<b>Amazon WorkDocs</b>	23/08/2022	186-190
10	<b>Managing Virtual Private Cloud</b>  A. Creating VPC in AWS Cloud B. Creating and Adding Private Subnet in the Existing VPC C. Deleting VPC	24/08/2022	191-196

## **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

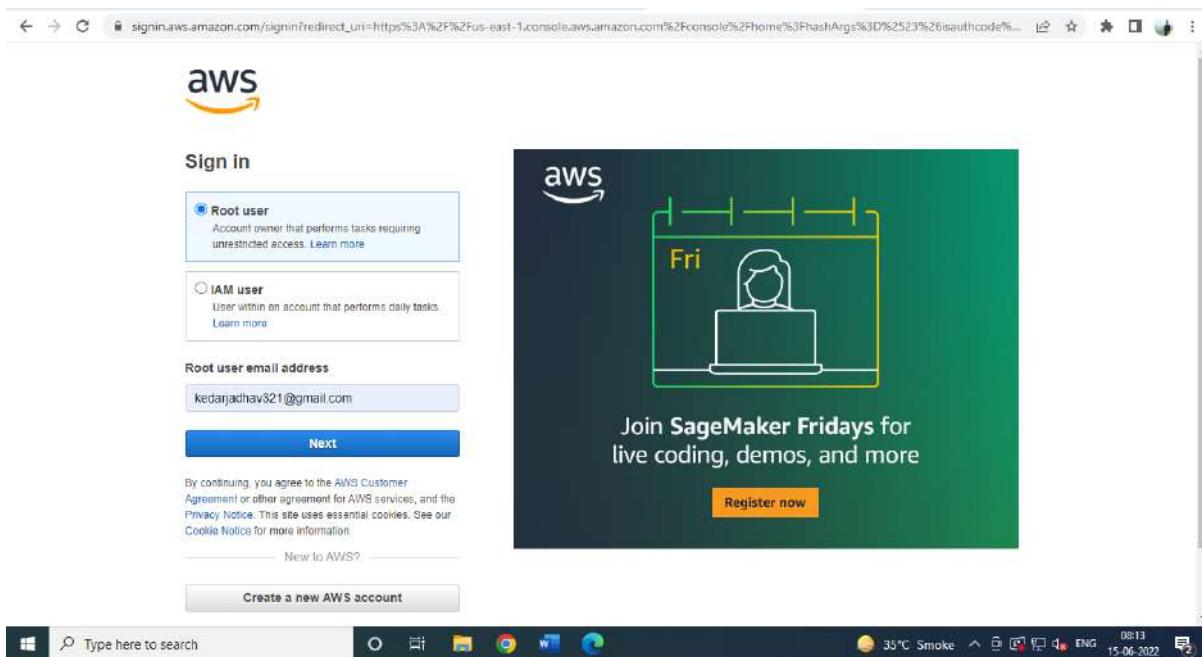
Head over to the Amazon Web Services website for Creating an AWS Account.

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.



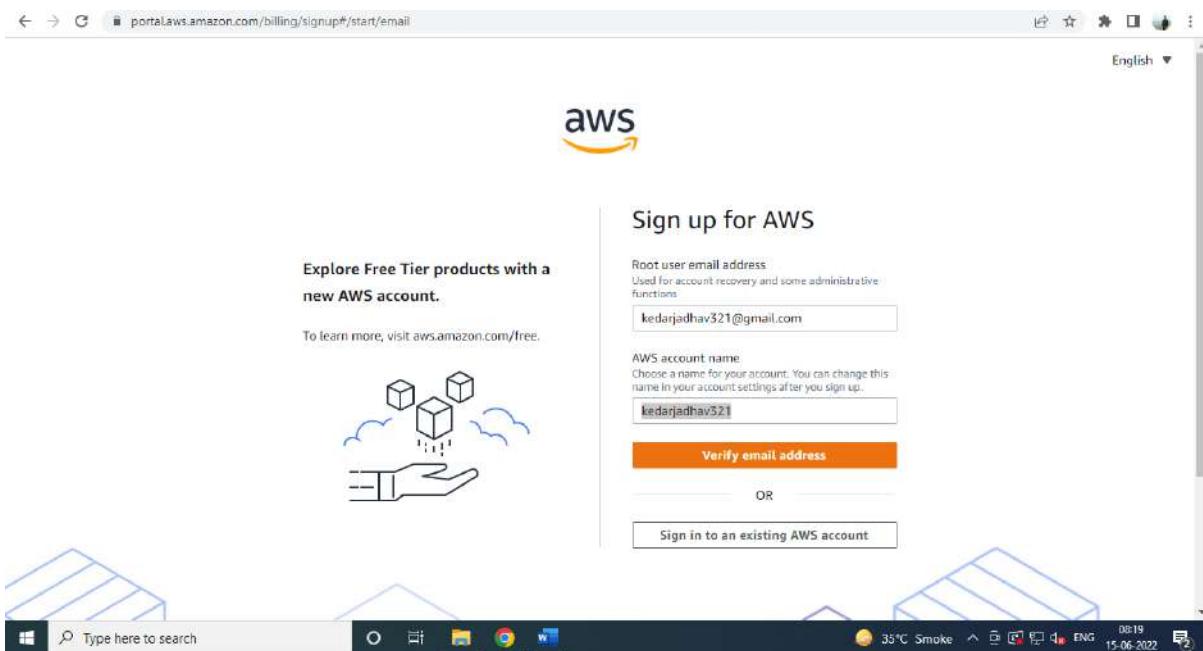
## Step 2: Entering User Details

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

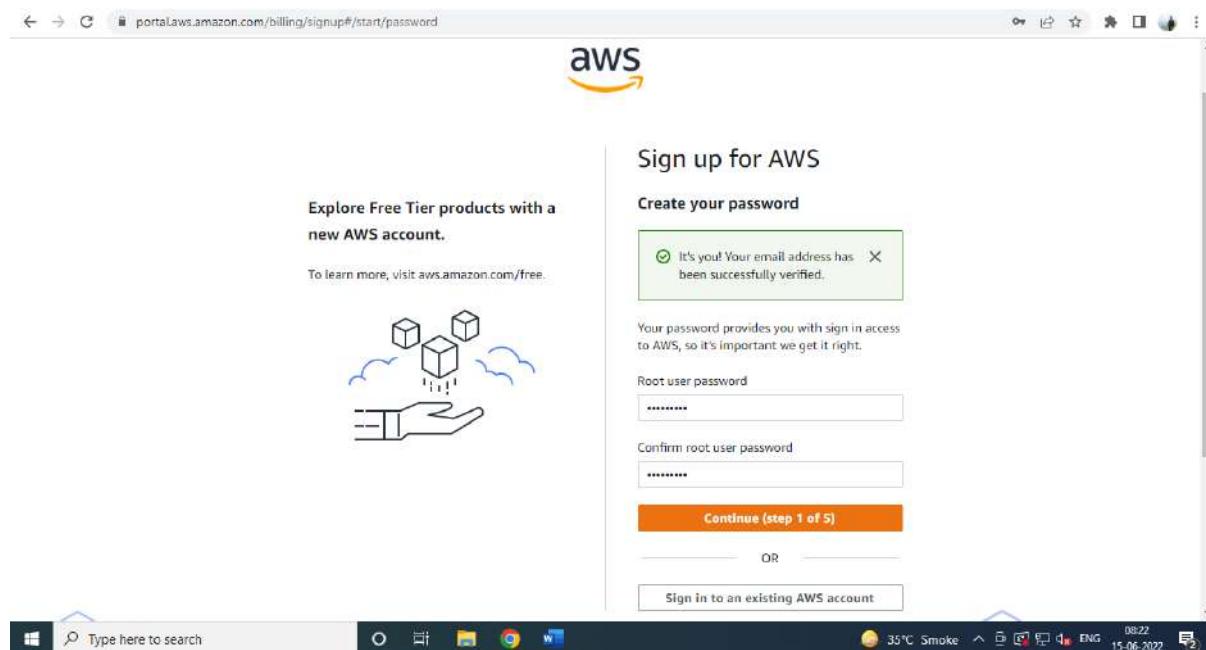
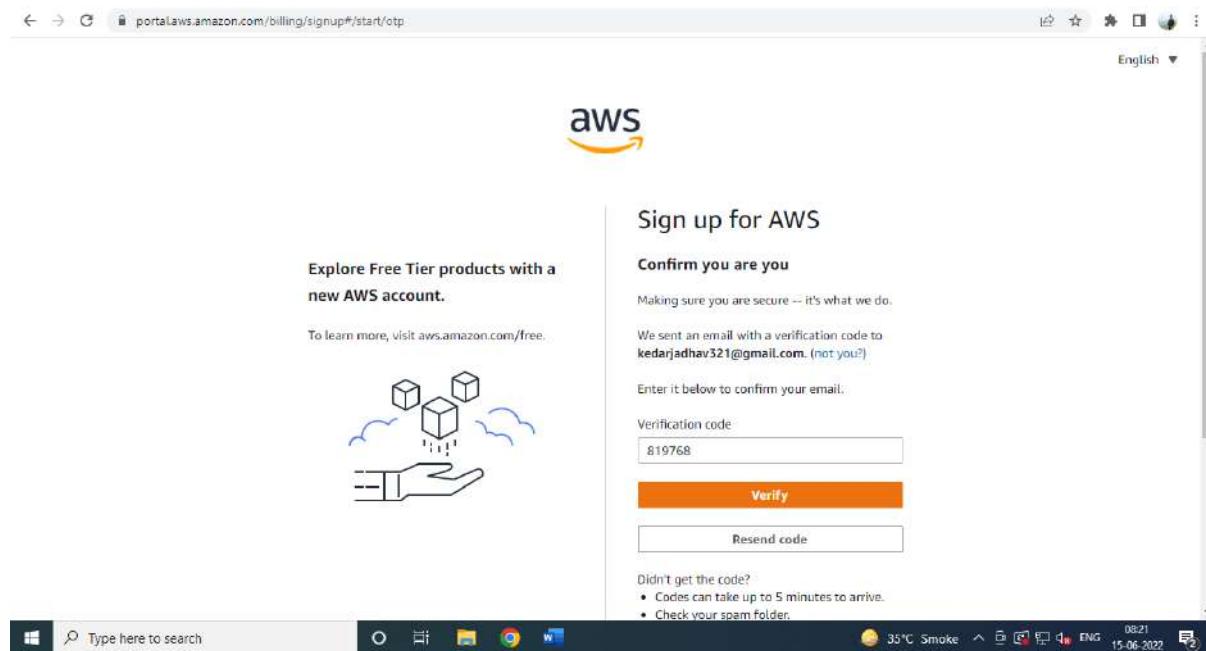
**Root user email Address:** [kedarjadhav321@gmail.com](mailto:kedarjadhav321@gmail.com)

**AWS Account Name:** `kedarjadhav321`

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.

### 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.

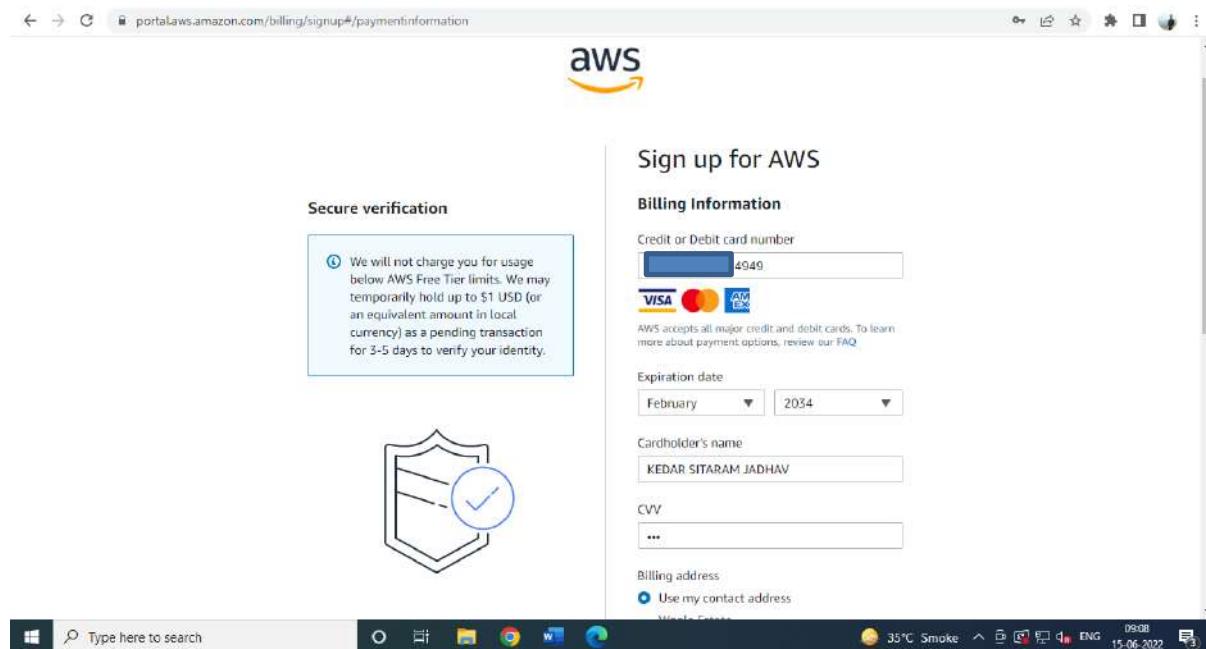
The screenshot shows the 'Sign up for AWS' page on the AWS portal. On the left, there's a section titled 'Free Tier offers' with three options: 'Always free' (never expires), '12 months free' (start from initial sign-up date), and 'Trials' (start from service activation date). On the right, the 'Contact Information' section is filled out with the following details:

Full Name	Kedar Sitaram Jadhav
Phone Number	9029108244
Country or Region	India
Address	Wagle Estate Thane
City	Thane
State, Province, or Region	Maharashtra
Postal Code	400604

At the bottom, there's a note about Indian contract addresses being served by AISPL, followed by a checked checkbox for accepting the AWS Customer Agreement, and a large orange 'Continue (step 2 of 5)' button.

#### 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.

**aws**

### Sign up for AWS

Select a support plan

Choose a support plan for your business or personal account. Compare plans and pricing examples

You can change your plan anytime in the AWS Management Console.

<input checked="" type="radio"/> Basic support - Free <ul style="list-style-type: none"><li>Recommended for individuals just getting started with AWS</li><li>24x7 self-service access to AWS resources</li><li>For account and AWS service usage</li><li>Access to Personal Health Dashboard &amp; Trusted Advisor</li></ul>	<input type="radio"/> Developer support - From \$29/month <ul style="list-style-type: none"><li>Recommended for developers programming with AWS</li><li>Get access to AWS Support during Business Hours</li><li>12 Business Hour response times</li></ul>	<input type="radio"/> Business support - From \$100/month <ul style="list-style-type: none"><li>Recommended for running production workloads</li><li>24x7 TWT support via email, phone, and chat</li><li>1-hour response times</li><li>Plan of Trusted Advisor best-practice recommendations</li></ul>
---	---	--

Need Enterprise level support?  
From \$15,000 a month you will receive 15-minute response times and concierge-style experience with an assigned Technical Account Manager. Learn more 

**Complete sign up.**

English ▾

**aws**



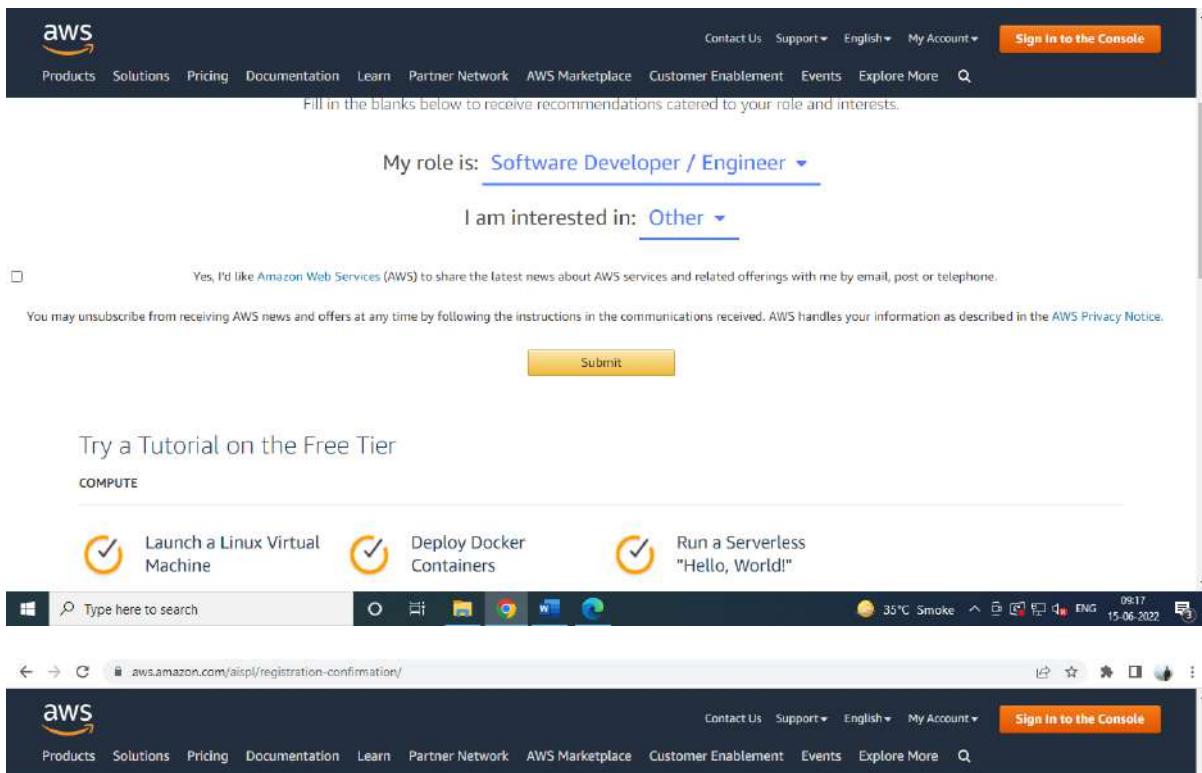
### Congratulations

Thank you for signing up for AWS.

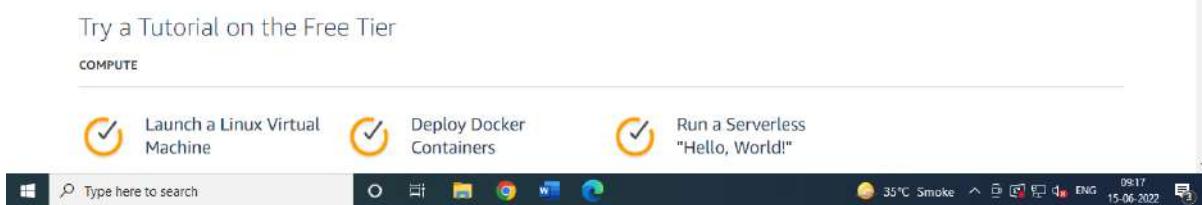
We are activating your account, which should only take a few minutes. You will receive an email when this is complete.

**Go to the AWS Management Console**

Sign up for another account or contact sales.



Thank You



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

The screenshot shows the AWS Home Page with the EC2 Dashboard selected. The left sidebar includes links for EC2 Dashboard, Events, Tags, Limits, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations), and Images. The main content area displays a summary of Amazon EC2 resources in the US East (N. Virginia) Region, showing 0 instances (running), 0 elastic IPs, 0 key pairs, 0 placement groups, and 0 snapshots. It also features a callout for launching Microsoft SQL Server Always On availability groups. To the right, the Account attributes section lists supported platforms (VPC), default VPC (vpc-0f52f94a7167cf0af), settings like EBS encryption and zones, and various AWS services. A 'Explore AWS' box provides tips for reducing AWS costs.

The screenshot shows the AWS Instances page for the us-east-1 region. The left sidebar is identical to the previous screenshot. The main content area shows a table header for Instances (Info) with columns: Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Availability Z. Below the table, a message states "No instances" and "You do not have any instances in this region". A "Launch instances" button is present. A modal window titled "Select an instance" is open at the bottom. The bottom of the screen shows the Windows taskbar with icons for File Explorer, Task View, File, Settings, Task Manager, and Edge browser.

The screenshot shows the AWS EC2 Dashboard under the 'New EC2 Experience'. The left sidebar includes links for EC2 Dashboard, Instances, and Images. The main content area shows the 'Scheduled events' section with 'No scheduled events' and the 'Migrate a server' section with a note about AWS Application Migration Service. The right sidebar features promotional banners for price performance and spot instances, and an 'Additional information' section with links to various AWS resources.

The screenshot shows the 'Launch an instance' page in the AWS EC2 Instances section. It includes fields for 'Name and tags', a search bar for 'Application and OS Images (Amazon Machine Image)', and a summary panel on the right containing details like the number of instances (1), software image (Amazon Linux 2 Kernel 5.10 AMI), virtual server type (t2.micro), and storage (1 volume(s) - 8 GiB). A red box highlights the 'Launch instance' button at the bottom right of the summary panel.

The screenshot shows the AWS EC2 Instances Launch Experience page. At the top, a success message indicates "Successfully initiated launch of Instance (i-07728b29dbbb8db8a)". Below this, there's a "Launch log" link. The "Next Steps" section includes links to "Get notified of estimated charges", "How to connect to your instance", and "View more resources". A prominent orange "View all Instances" button is at the bottom right.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 IP
-	i-07728b29dbbb8db8a	Running	t2.micro	Initializing	No alarms	ap-south-1a	ec2-13-126-18

The screenshot shows the AWS EC2 Instances page. The left sidebar is collapsed. The main area displays a table with one row of data, matching the details shown in the previous screenshot. An orange "Launch instances" button is visible at the top right of the table header.

## **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](#).

The screenshot shows the AWS EC2 Instances page. On the left sidebar, under the 'Instances' section, 'Instances' is selected. In the main content area, the heading 'Instances (1/1) Info' is displayed above a table. The table has one row for an instance named 'i-07728b29dbbb8db8a'. The instance is listed as 'Running' with the type 't2.micro'. The table includes columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 IP.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 IP
-	i-07728b29dbbb8db8a	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	ec2-13-126-18-62.ap-south-1.compute.amazonaws.com

Below the table, a detailed view for 'Instance: i-07728b29dbbb8db8a' is shown. The 'Details' tab is selected. Key details include:

- Instance summary:** Instance ID: i-07728b29dbbb8db8a, Public IPv4 address: 13.126.184.62, Private IPv4 address: 172.31.32.69.
- Hostname type:** IP name: ip-172-31-52-69.ap-south-1.compute.internal.
- Answer private resource DNS name:** IPv4 (A).
- Instance state:** Running.
- Private IP DNS name (IPv4 only):** ip-172-31-52-69.ap-south-1.compute.internal.
- Instance type:** t2.micro.
- Elastic IP addresses:** -.

This screenshot shows the 'Instance summary for i-07728b29dbbb8db8a' page. The left sidebar is identical to the previous screenshot. The main content area displays the same instance details as the previous screenshot, including the instance ID, public and private IP addresses, instance state, and instance type. Additionally, it shows the VPC ID (vpc-0b7cf751e125bb5cc), subnet ID (subnet-05312ac60a2bb9058), and IAM Role (-). A note at the bottom right suggests using the AWS Compute Optimizer for recommendations.

- **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

The screenshot shows the AWS Management Console interface for the EC2 service. On the left, there's a navigation sidebar with links like 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', 'Instances' (selected), 'Images', and 'Elastic Block Store'. The main content area displays a table of instances. One instance, 'i-07728b29dbbb8db8a', is selected and its details are shown in a modal window. The 'Security' tab is active in the modal, showing the following information:

Security group rule ID	Port range	Protocol	Source	Security groups
				sg-01a3358612c289bff [Launch-wizard-1]

Below the modal, the taskbar shows system icons for battery, signal, and date/time (05:54 PM, 15-06-2022).

## 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 IAM 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

Introduction to AWS Identity and Access Management (IAM)

00:45:00

Provisioning lab resources  
Est. time remaining: Less than 1 minute

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. [Learn more](#)

45 minutes Free Rate Lab

aws training and certification

SPL-66 - version 3.1.14

© 2022 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. All trademarks are the property of their owners.

28°C Rain off and on ENG IN 08:08 PM 24-06-2022

Introduction to AWS Identity and Access Management (IAM)

00:44:36

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. [Learn more](#)

Open Console

Subscribed

arn:40977654-585034ac:

Username

I-Ba1373262baBa1516

AdministratorAccess

xTBux1!NgSaf53x

Region

us-west-2

45 minutes Free Rate Lab

aws training and certification

SPL-66 - version 3.1.14

© 2022 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. All trademarks are the property of their owners.

28°C Rain off and on ENG IN 08:08 PM 24-06-2022

**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.**

The screenshot shows the AWS Management Console homepage. The navigation bar includes links for AWS services like S3, EC2, and IAM. A prominent banner at the top right informs users that the new AWS Console Home will replace the existing experience soon, starting in June 2022. It includes a 'Switch now' button and a link to learn more. Another section below it promotes the AWS Console Mobile App, which supports four additional regions and can be downloaded to iOS or Android devices.

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

The screenshot shows the IAM Management Console dashboard. The left sidebar has 'Identity and Access Management (IAM)' expanded, with 'Users' selected. The main area shows the 'IAM dashboard' with the following resource counts: 4 User groups, 5 Users, 19 Roles, 2 Policies, and 0 Identity providers. A 'What's new' section highlights updates for features in IAM, such as Right-size permissions for more roles and Amazon S3 Object Ownership. The 'Tools' section includes links to 'Policy simulator' and 'Web identity federation playground'.

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

- user-1
- user-2

- User-3

The screenshot shows the AWS IAM Management Console with the 'Users' list page. The left sidebar shows navigation options like Dashboard, Access management, and Access reports. The main area displays a table of users:

User name	Groups	Last activity	MFA	Password age	Active key age
awstudent	QLReadOnly	Never	None	5 minutes ago	5 minutes ago
root-qwkl	None	Never	None	-	-
user-1	None	Never	None	4 minutes ago	-
user-2	None	Never	None	4 minutes ago	-
user-3	None	Never	None	4 minutes ago	-

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

The screenshot shows the AWS IAM Management Console with the 'Summary' page for the 'user-1' user. The left sidebar shows navigation options like Dashboard, Access management, and Access reports. The main area displays user details and navigation tabs:

- Permissions
- Groups
- Tags (2)
- Security credentials
- Access Advisor

Below the tabs, there's a 'Permissions policies' section with a 'Get started with permissions' message and 'Add permissions' and 'Add inline policy' buttons. At the bottom, there's a 'Permissions boundary (not set)' section.

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

User ARN: arn:aws:iam::566451885690:user/spl66/user-1  
Path: /spl66/  
Creation time: 2022-06-24 20:06 UTC+0530

**Permissions** **Groups** **Tags (2)** **Security credentials** **Access Advisor**

**Permissions policies**

Get started with permissions  
This user doesn't have any permissions yet. Get started by adding the user to a group, copying permissions from another user, or attaching a policy directly. Learn more

Add permissions **Add inline policy**

Permissions boundary (not set)

Generate policy based on CloudTrail events  
You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

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

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

Users > user-1

**Summary**

User ARN: arn:aws:iam::566451885690:user/spl66/user-1  
Path: /spl66/  
Creation time: 2022-06-24 20:06 UTC+0530

**Permissions** **Groups** **Tags (2)** **Security credentials** **Access Advisor**

Add user to groups

Group name	Attached permissions
	No results

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

The screenshot shows the AWS IAM Management Console for a user named 'user-1'. The 'Security credentials' tab is selected. Under 'Sign-in credentials', it shows:

- Console password: Enabled (never signed in) | Manage
- Assigned MFA device: Not assigned | Manage
- Signing certificates: None

Below this, there is information about access keys and a note about protecting secret keys.

**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

The screenshot shows the 'User groups' page in the AWS IAM Management Console. It lists the following groups:

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	7 minutes ago
EC2-Support	0	Defined	7 minutes ago
QLReadOnly	1	Defined	7 minutes ago
S3-Support	0	Defined	7 minutes ago

**Step 11 – Click the EC2-Support group.**

The screenshot shows the AWS IAM Management Console with the URL <https://us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/EC2-Support?section=users>. The page displays the 'EC2-Support' user group details. The 'Summary' section shows the user group name 'EC2-Support', creation time 'June 24, 2022, 20:06 (UTC+05:30)', and ARN 'arn:aws:iam::566451885690:group/spl60/EC2-Support'. Below the summary, there are tabs for 'Users', 'Permissions', and 'Access Advisor'. The 'Users' tab is selected, showing a table with columns 'User name', 'Groups', 'Last activity', and 'Creation time'. A search bar and filter buttons are also present. The 'Permissions' tab is visible but not selected. The left sidebar shows navigation options like 'Dashboard', 'Access management (User groups, Users, Roles, Policies, Identity providers, Account settings)', 'Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs))', and 'Feedback'.

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

**Step 11 – Click the Permissions tab.**

The screenshot shows the AWS IAM Management Console with the URL <https://us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/EC2-Support?section=permissions>. The page displays the 'EC2-Support' user group details. The 'Summary' section shows the user group name 'EC2-Support', creation time 'June 24, 2022, 20:06 (UTC+05:30)', and ARN 'arn:aws:iam::566451885690:group/spl60/EC2-Support'. Below the summary, there are tabs for 'Users', 'Permissions', and 'Access Advisor'. The 'Permissions' tab is selected, showing a table with columns 'Policy name', 'Type', and 'Description'. A search bar and filter buttons are also present. One policy named 'AmazonEC2ReadOnlyAccess' is listed under the 'AWS managed' type. The left sidebar shows navigation options like 'Dashboard', 'Access management (User groups, Users, Roles, Policies, Identity providers, Account settings)', 'Access reports (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs))', and 'Feedback'.

This group has a Managed Policy associated with it, called **AmazonEC2ReadOnlyAccess**. 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 12 – Under Actions, click the Show Policy link.**

```

1 "Version": "2012-10-17",
2 "Statement": [
3     {
4         "Effect": "Allow",
5         "Action": "ec2:Describe*",
6         "Resource": "*"
7     },
8     {
9         "Effect": "Allow",
10        "Action": "elasticloadbalancing:Describe",
11        "Resource": "*"
12    },
13    {
14        "Effect": "Allow",
15        "Action": [
16            "cloudwatch:ListMetrics",
17            "cloudwatch:GetMetricStatistics",
18            "cloudwatch:Describe"
19        ],
20        "Resource": "*"
21    },
22    {
23        "Effect": "Allow",
24        "Action": "autoScaling:Describe",
25        "Resource": "*"
26    }
27 ],
28 }
29 ]

```

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.**

The screenshot shows the IAM Management Console with the URL <https://us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/EC2-Support?section=permissions>. The left sidebar is collapsed. The main content area shows the 'EC2-Support' user group under 'User groups'. The 'Permissions' tab is active, showing a single policy named 'AmazonEC2ReadOnlyAccess' attached. The policy is described as 'Provides read only access to Am'.

**Step 15 – Click the S3-Support Group.**

The screenshot shows the IAM Management Console with the URL <https://us-east-1.console.aws.amazon.com/iamv2/home#/groups>. The left sidebar is collapsed. The main content area shows the 'User groups' page with four groups listed: EC2-Admin, EC2-Support, QLReadOnly, and S3-Support. The S3-Support group has the 'AmazonS3ReadOnlyAccess' policy attached, as indicated by the green checkmark icon in the 'Permissions' column.

The S3-Support group has the AmazonS3ReadOnlyAccess policy attached.

Policy name	Type	Description
AmazonS3ReadOnlyAccess	AWS managed	Provides read only access to all b

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

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	14 minutes ago
EC2-Support	0	Defined	14 minutes ago
QLReadOnly	1	Defined	14 minutes ago
S3-Support	0	Defined	14 minutes ago

**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 an Inline 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

The screenshot shows the AWS IAM Management Console interface. On the left, there's a navigation sidebar with options like 'Access management', 'User groups', 'Users', 'Roles', 'Policies', etc. The main area shows the 'EC2-Admin' user group details. The 'Permissions' tab is active, showing a single inline policy named 'EC2-Admin-Policy'. The policy document is displayed as follows:

```

1 "Version": "2012-10-17",
2 "Statement": [
3     {
4         "Action": [
5             "ec2:Describe*",
6             "ec2:StartInstances",
7             "ec2:StopInstances",
8             "cloudwatch:DescribeAlarms"
9         ],
10        "Resource": [
11            "*"
12        ],
13        "Effect": "Allow"
14    }
]
  
```

The screenshot shows the AWS IAM Management Console interface. The left sidebar is identical to the previous screenshot. The main area shows the 'EC2-Admin' user group details. The 'Permissions' tab is active, showing a single inline policy named 'EC2-Admin-Policy'. The policy document is displayed as follows:

```

1 "Version": "2012-10-17",
2 "Statement": [
3     {
4         "Action": [
5             "ec2:Describe*",
6             "ec2:StartInstances",
7             "ec2:StopInstances",
8             "cloudwatch:DescribeAlarms"
9         ],
10        "Resource": [
11            "*"
12        ],
13        "Effect": "Allow"
14    }
]
  
```

The screenshot shows the AWS IAM Management Console with the URL [https://us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/EC2-Admin\)section=permissions](https://us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/EC2-Admin)section=permissions). The left sidebar shows 'User groups' with 'EC2-Admin' selected. The main area is titled 'Permissions policies (1)' and displays the 'EC2-Admin-Policy'. The policy document is shown in JSON format:

```

1  {
2    "Version": "2012-10-17",
3    "Statement": [
4      {
5        "Action": [
6          "ec2:Describe",
7          "ec2:StartInstances",
8          "ec2:StopInstances",
9          "cloudwatch:DescribeAlarms"
10       ],
11       "Resource": [
12         "*"
13       ],
14       "Effect": "Allow"
15     }
16   ]
17 }
```

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**

The screenshot shows the 'Edit EC2-Admin-Policy' page. The URL is [https://us-east-1.console.aws.amazon.com/iam/home#/policies\\$inlineEdit?groupID=EC2-Admin&policyName=EC2-Admin-Policy&step=edit](https://us-east-1.console.aws.amazon.com/iam/home#/policies$inlineEdit?groupID=EC2-Admin&policyName=EC2-Admin-Policy&step=edit). The left sidebar shows 'Documentation'. The main area has tabs for 'Visual editor' (selected) and 'JSON'. It lists actions under 'EC2 (136 actions)' and 'CloudWatch (1 action)'. At the bottom, it says 'Character count: 170 of 5,120' and 'The current character count includes character for all inline policies in this group: EC2-Admin.' There are 'Cancel' and 'Review policy' buttons.

**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 Amazon EC2 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

The screenshot shows the AWS IAM Management Console. The left sidebar has 'User groups' selected under 'Access management'. The main area shows the 'EC2-Support' group details. The 'Summary' tab is selected, showing the group name 'EC2-Support', creation time 'June 24, 2022, 20:06 (UTC+05:30)', and ARN 'arn:aws:iam::566451885690:group/spl6/EC2-Support'. Below this, the 'Users' tab is selected, showing a table with columns 'User name', 'Groups', 'Last activity', and 'Creation time'. A search bar and filters are at the top of the table. At the bottom of the page, there are links for 'Feedback', 'Language selection', 'Privacy', 'Terms', and 'Cookie preferences', along with system status icons like battery level and network connection.

**Step 23 – Click the S3-Support group.**

Group name	Users	Permissions	Creation time
EC2-Admin	0	0	18 minutes ago
EC2-Support	0	0	18 minutes ago
QLReadOnly	0	0	18 minutes ago
S3-Support	0	0	18 minutes ago

### 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.

The screenshot shows the AWS IAM Management Console. On the left, the navigation pane is open with 'User groups' selected under 'Access management'. The main area shows a table titled 'Other users in this account (Selected 1/5)' with columns for 'User name', 'Groups', 'Last activity', and 'Creation time'. One user, 'user-1', is selected, indicated by a blue border around the row. At the bottom right of the table, there are 'Cancel' and 'Add users' buttons.

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

The screenshot shows the AWS IAM Management Console. The left navigation pane is identical to the previous screenshot. The main area is titled 'S3-Support' and includes a 'Summary' section with details like 'User group name: S3-Support', 'Creation time: June 24, 2022, 20:06 (UTC+05:30)', and 'ARN: arn:aws:iam::566451885690:group/spl6/S3-Support'. Below this is a 'Users' tab, which is active, showing a table with one entry: 'User name: user-1'. There are 'Edit', 'Delete', 'Remove users', and 'Add users' buttons at the top of this section. The status bar at the bottom indicates the date and time as '24-06-2022 08:27 PM'.

## 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.

The screenshot shows the AWS IAM Management Console with the URL <https://us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/S3-Support?section=users>. The page displays the 'S3-Support' user group under the 'User groups' section. The 'Summary' tab is selected, showing the group name 'S3-Support', creation time 'June 24, 2022, 20:06 (UTC+05:30)', and ARN 'arn:aws:iam::566451885690:group/splb6/S3-Support'. Below this, the 'Users' tab is selected, showing one user named 'user-1' added to the group. The user has 1 group, last activity 'None', and was created 20 minutes ago. There are buttons for 'Edit' and 'Delete' at the top right of the summary section.

## 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.

Group name	Users	Permissions	Creation time
EC2-Admin	1	Loading	21 minutes ago
EC2-Support	0	Loading	21 minutes ago
QLReadOnly	0	Loading	21 minutes ago
S3-Support	1	Loading	21 minutes ago

## 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.

User group name	Creation time	ARN
EC2-Support	June 24, 2022, 20:06 (UTC+05:30)	arn:aws:iam::566451885690:group/spl66/EC2-Support

The screenshot shows the AWS IAM Management Console interface. The left sidebar navigation includes 'Identity and Access Management (IAM)', 'Access management' (with 'User groups' selected), 'Access reports', and other options like 'Roles', 'Policies', and 'Service control policies (SCPs)'. The main content area is titled 'Add users to EC2-Support' and displays a table of 'Other users in this account' (Selected 1/5). The table columns are 'User name', 'Groups', 'Last activity', and 'Creation time'. The users listed are 'awsstudent', 'root-qwkl', 'user-1', 'user-2' (which is selected with a checked checkbox), and 'user-3'. At the bottom right of the table are 'Cancel' and 'Add users' buttons.

The screenshot shows the 'EC2-Support' group summary page. The top message says 'Users added to this group.' Below it, the group details are shown: 'User group name: EC2-Support', 'Creation time: June 24, 2022, 20:06 (UTC+05:30)', and 'ARN: arn:aws:iam::506451885690:group/spl00/EC2-Support'. The 'Users' tab is selected, showing a table of users in the group. The table columns are 'User name', 'Groups', 'Last activity', and 'Creation time'. The user 'user-2' is listed. At the bottom right of the table are 'Delete', 'Edit', 'Remove users', and 'Add users' buttons.

The screenshot shows the AWS IAM Management Console with the URL <https://us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/EC2-Support?section=users>. The left navigation pane is open, showing 'User groups' under 'Access management'. The main content area displays the 'EC2-Support' user group. The 'Summary' tab is selected, showing the group name 'EC2-Support', creation time 'June 24, 2022, 20:06 (UTC+05:30)', and ARN 'arn:aws:iam::566451885690:group/spl6/EC2-Support'. Below this, there are tabs for 'Users', 'Permissions', and 'Access Advisor'. Under the 'Users' tab, it says 'Users in this group (1)'. A table lists one user: 'user2' (User name), 'None' (Groups), '22 minutes ago' (Last activity), and '22 minutes ago' (Creation time). There are buttons for 'Edit', 'Delete', 'Remove users', and 'Add users'. The status bar at the bottom shows 'ENG IN' and the date '24-06-2022'.

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

The screenshot shows the AWS IAM Management Console with the URL <https://us-east-1.console.aws.amazon.com/iamv2/home#/groups>. The left navigation pane is open, showing 'User groups' under 'Access management'. The main content area displays the 'User groups' page. It says 'User groups (4)'. A table lists four groups: 'EC2-Admin', 'EC2-Support', 'QLReadOnly', and 'S3-Support'. Each row includes columns for 'Group name', 'Users', 'Permissions', and 'Creation time'. Buttons for 'Delete' and 'Create group' are visible. The status bar at the bottom shows 'ENG IN' and the date '24-06-2022'.

**EC2-Admin**

**Summary**

User group name	EC2-Admin	Creation time	June 24, 2022, 20:06 (UTC+06:30)
		ARN	arn:aws:iam::566451885690:group/splB6/EC2-Admin

**Users**    **Permissions**    **Access Advisor**

**Users in this group (0)** info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

**Add users**

No resources to display

**Add users to EC2-Admin**

**Other users in this account (Selected 1/5)** info

User name	Groups	Last activity	Creation time
awsstudent	1	None	4 years ago
root-qwkl	You need permissions	None	4 years ago
user-1	1	None	22 minutes ago
user-2	1	None	22 minutes ago
<input checked="" type="checkbox"/> user-3	0	None	22 minutes ago

**Add users**

The screenshot shows the AWS IAM Management Console interface. The main title bar reads "Introduction to AWS Identity and IAM Management Console". The URL is <https://us-east-1.console.aws.amazon.com/iamv2/home#/groups/details/EC2-Admin?section=users>. The top navigation bar includes links for "Gmail", "YouTube", "Bookmarks", "Search for services, features, blogs, docs, and more [Alt+S]", "Global", and "awsstudent @ 5664-5188-5690".

The left sidebar menu is expanded under "Access management" with "User groups" selected. Other options include "Users", "Roles", "Policies", "Identity providers", and "Account settings". Under "Access reports", "Archive rules", "Analyzers", and "Settings" are listed.

The main content area displays the "EC2-Admin" user group summary. It shows the group name "EC2-Admin", creation time "June 24, 2022, 20:06 (UTC+05:30)", and ARN "arn:aws:iam::566451885690:group/spl60/EC2-Admin". There are tabs for "Users", "Permissions", and "Access Advisor".

The "Users" tab shows a table with one row for "user-3". The table columns are "User name", "Groups", "Last activity", and "Creation time". The "user-3" entry shows "1" under Groups, "None" under Last activity, and "23 minutes ago" under Creation time. Buttons for "Remove users" and "Add users" are present.

The status bar at the bottom indicates "Feedback", "Looking for language selection? Find it in the new Unified Settings", "© 2022, Amazon Web Services, Inc. or its affiliates.", "Privacy", "Terms", "Cookie preferences", "ENG IN", "Rain off and on", "08:30 PM", "24-06-2022", and a battery icon.

Group name	Users	Permissions	Creation time
EC2-Admin	1	↳ Loading	24 minutes ago
EC2-Support	1	↳ Loading	24 minutes ago
QLReadOnly	↳ Loading	↳ Loading	24 minutes ago
S3-Support	1	↳ Loading	24 minutes ago

Group name	Users	Permissions	Creation time
EC2-Admin	1	↗ Loading	24 minutes ago
EC2-Support	1	↗ Loading	24 minutes ago
QLReadOnly	↗ Loading	↗ Loading	24 minutes ago
S3-Support	1	↗ Loading	24 minutes ago

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

**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.**

**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.

The screenshot shows the IAM dashboard with the following statistics:

User groups	Users	Roles	Policies	Identity providers
4	5	19	2	0

**Security recommendations:**

- Add MFA for root user

**What's new:**

- Right-size permissions for more roles in your account using IAM Access Analyzer to generate 50 fine-grained IAM policies per day. 7 months ago
- Amazon S3 Object Ownership can now disable access control lists to simplify access management for data in S3. 7 months ago
- Amazon Redshift simplifies the use of other AWS services by introducing the default IAM role. 7 months ago
- IAM Access Analyzer helps you generate fine-grained policies that specify the required actions for more than 60 services. 10 months ago

**Tools:**

- Policy simulator
- Web identity federation playground

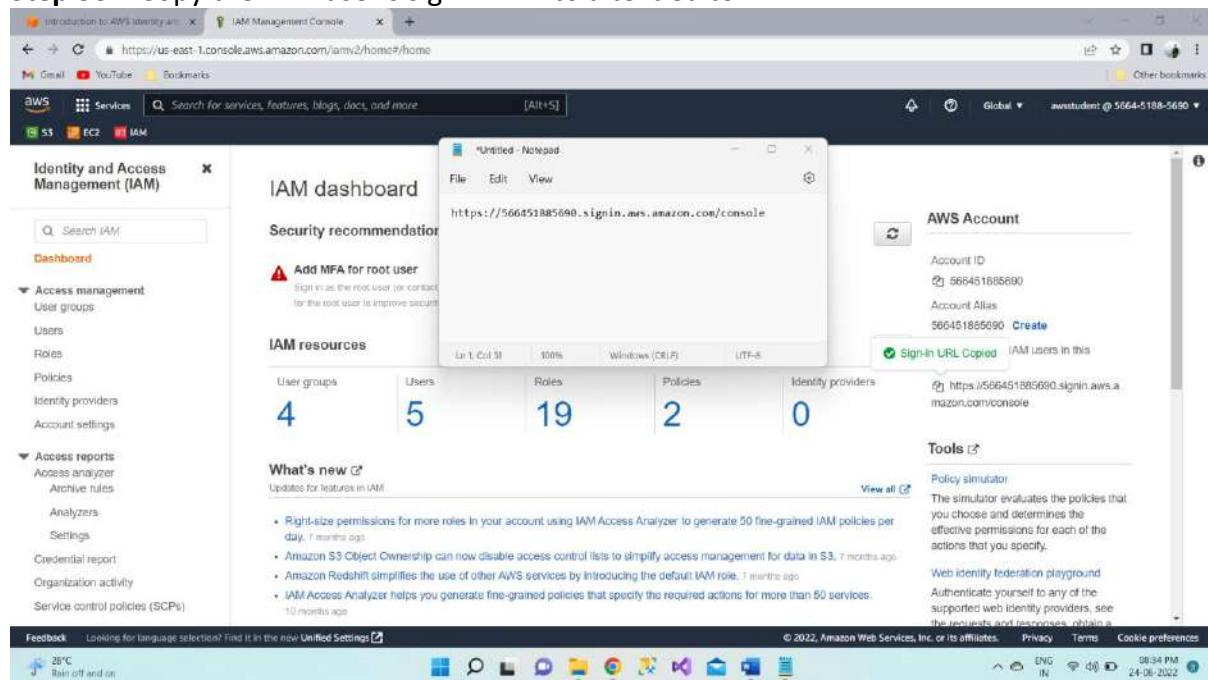
An IAM users sign-in link is displayed It will look similar to:

<https://566451885690.signin.aws.amazon.com/console>

The screenshot shows the IAM dashboard with the same statistics as before. A message 'Sign-In URL Copied' is displayed in the top right corner of the 'AWS Account' section, indicating the sign-in URL has been copied to the clipboard.

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.



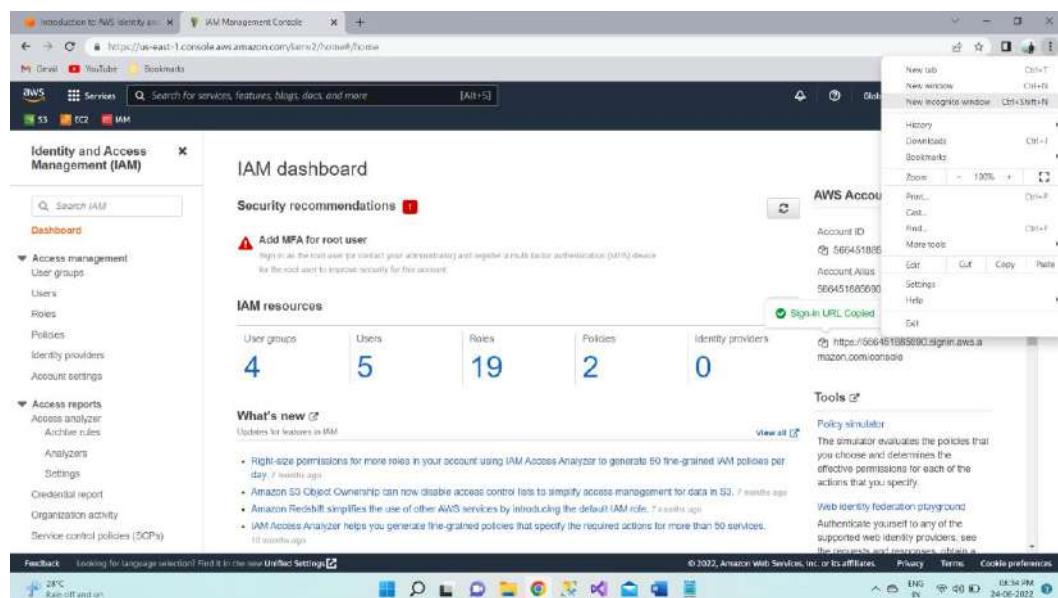
### Step 31 – Open a private window.

#### 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



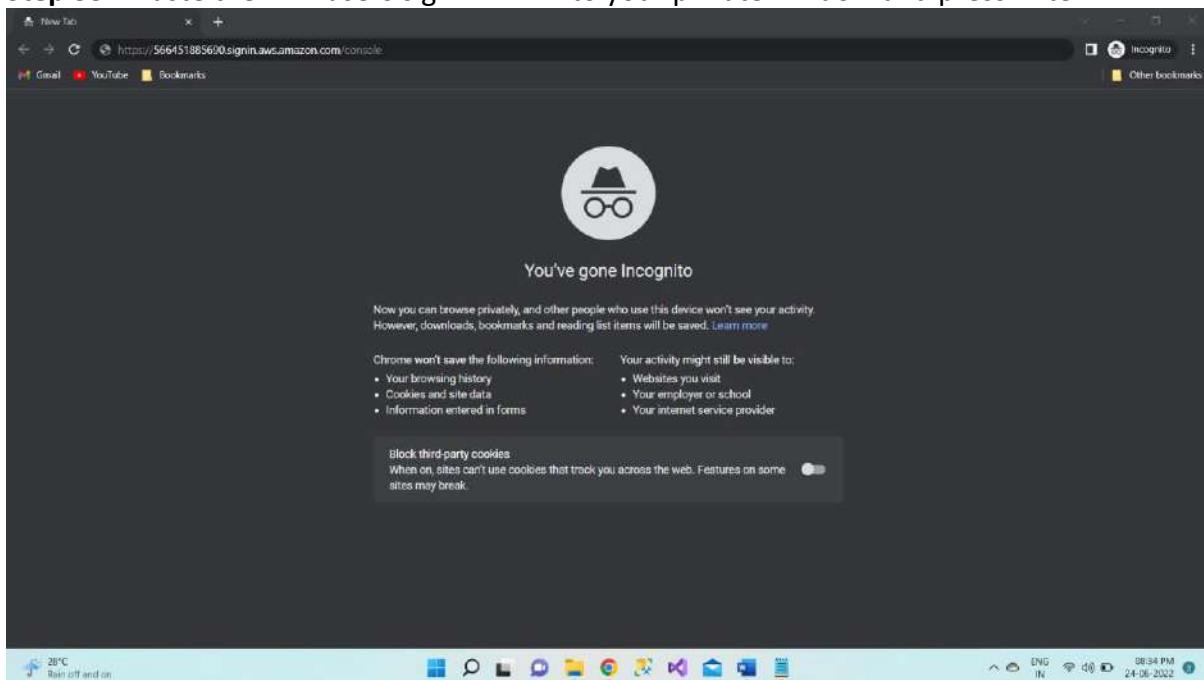
## Microsoft Edge

- 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.

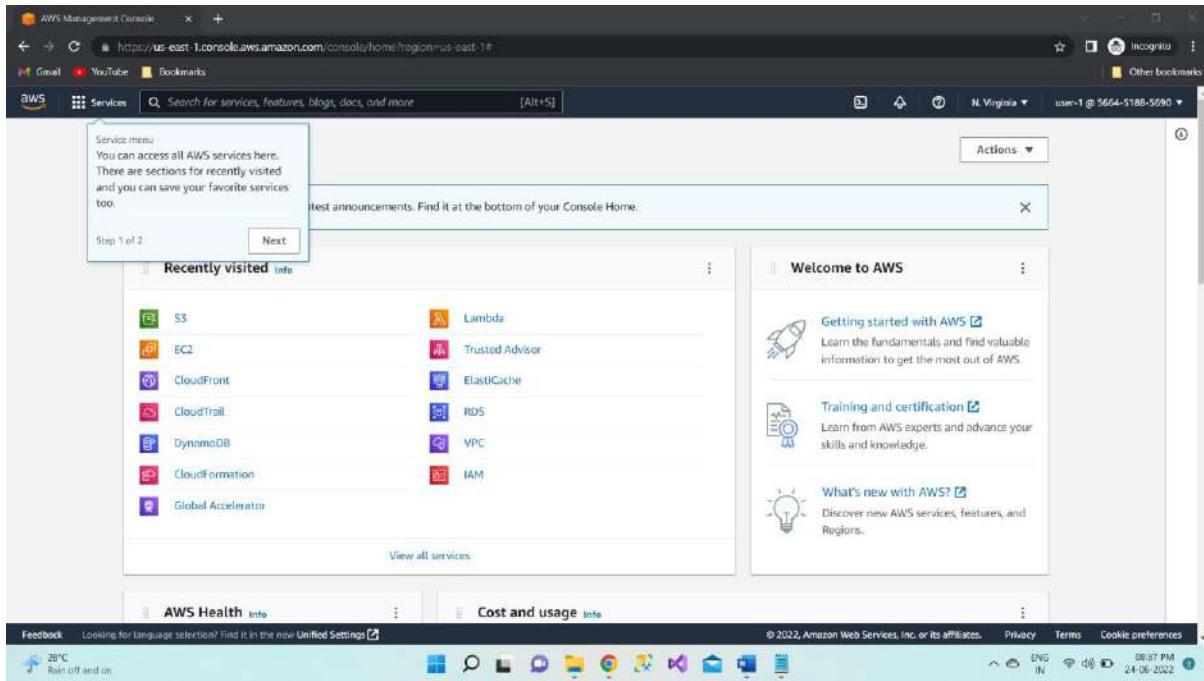
**Step 34** – Sign-in with: IAMusername: user-1

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

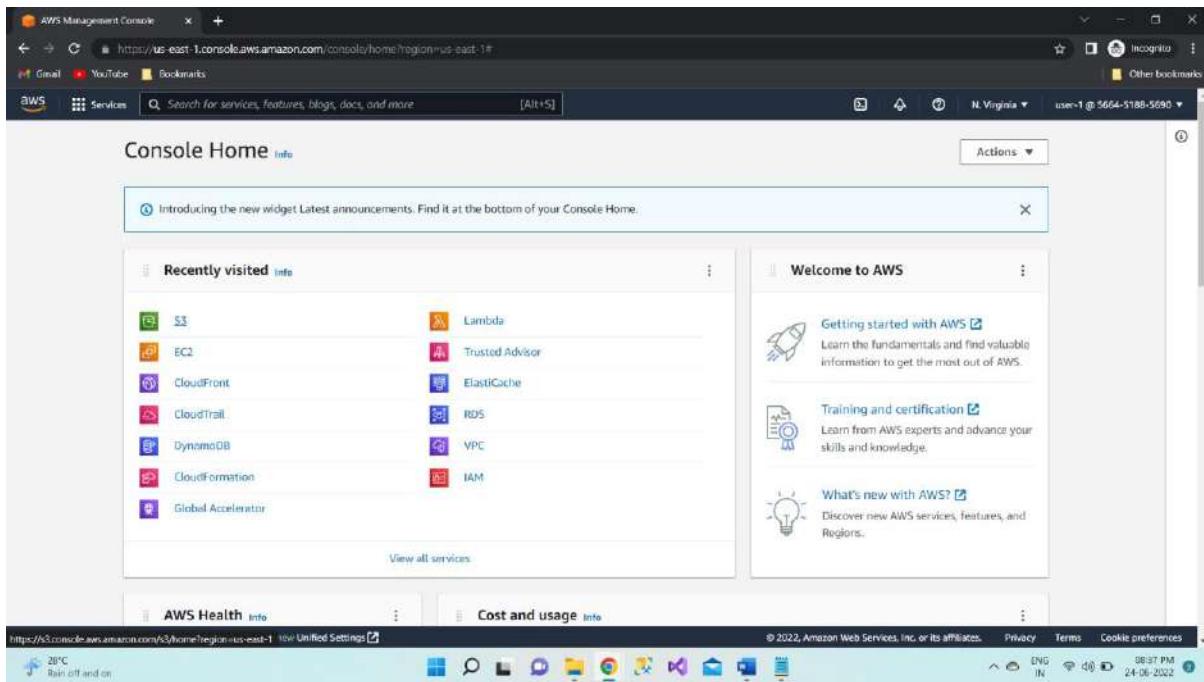
The screenshot shows the AWS Sign-in page at [https://signin.aws.amazon.com/oauth?client\\_id=amzn1%2wave%3Asignin%3A%3Aconsole%2Fcanvas&code\\_challenge=BmvlPkjWfzsq\\_ekUimTc8og875V\\_ZH6qqeqI&code\\_challenge\\_type=sha256](https://signin.aws.amazon.com/oauth?client_id=amzn1%2wave%3Asignin%3A%3Aconsole%2Fcanvas&code_challenge=BmvlPkjWfzsq_ekUimTc8og875V_ZH6qqeqI&code_challenge_type=sha256). The page includes fields for Account ID, IAM user name, Password, and a Remember this account checkbox. A blue "Sign in" button is prominent. To the right, there's a dark banner with the text "Expanded Databases Free Tier" and "Start today for free including DocumentDB, Neptune, additional RDS instances, and more!" with a "LEARN MORE" button.

The screenshot shows the IAM Management Console at [https://amazon.qwiklabs.com/focuses/22172/catalog\\_rank=%7B%22rank%22%3A1%2C%22num\\_filters%22%3A0%2C%22has\\_search%22%3Atrue%2C%22parent%22%3Acatalog&search\\_id=14619834](https://amazon.qwiklabs.com/focuses/22172/catalog_rank=%7B%22rank%22%3A1%2C%22num_filters%22%3A0%2C%22has_search%22%3Atrue%2C%22parent%22%3Acatalog&search_id=14619834). The page title is "Introduction to AWS Identity and Access Management (IAM)". It features a large heading "Introduction to AWS Identity and Access Management (IAM)", a "Rate Lab" section with a 5-star rating, and a "SPL-66 - version 3.1.14" note. On the left, there's a sidebar with links like "Open Console", "s3Bucket01", "Instances01", "AdministratorPassword", and "Region". On the right, there's a sidebar with sections like "Lab Overview", "Topics covered", "Start Lab", "Task 1: Explore the Users and Groups", "Business Scenario", "Task 2: Add Users to Groups", "Task 3: Sign-in and Test Users", "End Lab", "Conclusion", and "Additional Resources".



**Step 35 – In the Services menu, click S3.**



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

The screenshot shows the AWS S3 Management Console. On the left, a sidebar navigation includes 'Buckets', 'Storage Lens', and 'AWS Marketplace for S3'. The main content area displays an 'Account snapshot' with metrics: Total storage (128.9 KB), Object count (46), and Avg. object size (2.8 KB). Below this is a table titled 'Buckets (3) Info' showing three buckets:

Name	AWS Region	Access	Creation date
ql-cf-templates-1656081394-490beefc12487f5-us-west-2	US West (Oregon) us-west-2	Objects can be public	June 24, 2022, 20:06:37 (UTC+05:30)
qls-48977654-5853634ac795fd1a-s3bucket-19bjwvx9pjpv	US West (Oregon) us-west-2	Objects can be public	June 24, 2022, 20:06:44 (UTC+05:30)
qltrial-lab-4134-1656081398	US East (N. Virginia) us-east-1	Objects can be public	June 24, 2022, 20:06:40 (UTC+05:30)

This screenshot shows the same AWS S3 Management Console interface. The 'Buckets' table now lists four buckets:

Name	AWS Region	Access	Creation date
ql-cf-templates-1656081394-490beefc12487f5-us-west-2	US West (Oregon) us-west-2	Objects can be public	June 24, 2022, 20:06:37 (UTC+05:30)
qls-48977654-5853634ac795fd1a-s3bucket-19bjwvx9pjpv	US West (Oregon) us-west-2	Objects can be public	June 24, 2022, 20:06:44 (UTC+05:30)
qltrial-lab-4134-1656081398	US East (N. Virginia) us-east-1	Objects can be public	June 24, 2022, 20:06:40 (UTC+05:30)
ql-cf-templates-1656081394-490beefc12487f5-us-east-1	US East (N. Virginia) us-east-1	Objects can be public	June 24, 2022, 20:06:37 (UTC+05:30)

**Amazon S3**

**Buckets**

- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- Access analyzer for S3

Block Public Access settings for this account

▼ Storage Lens

- Dashboards
- AWS Organizations settings

Feature spotlight: (1)

► AWS Marketplace for S3

**ql-cf-templates-1656081394-4908ee8fcf2487f5-us-west-2**

**Objects (1)**

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Name	Type	Last modified	Size	Storage class
lab-4134.json	json	June 24, 2022, 20:06:37 (UTC+05:30)	4.3 KB	Standard

**Feedback** Looking for language selection? Find it in the new [Unified Settings](#)

28°C Rain off and on

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 08:49 PM 24-06-2022

**Amazon S3**

**Properties**

**Object overview**

Owner	s3://ql-cf-templates-1656081394-4908ee8fcf2487f5-us-west-2/lab-4134.json
AWS Region	US West (Oregon) us-west-2
Last modified	June 24, 2022, 20:06:37 (UTC+05:30)
Size	4.3 KB
Type	json
Key	https://ql-cf-templates-1656081394-4908ee8fcf2487f5-us-west-2.s3.amazonaws.com/lab-4134.json

**Feedback** Looking for language selection? Find it in the new [Unified Settings](#)

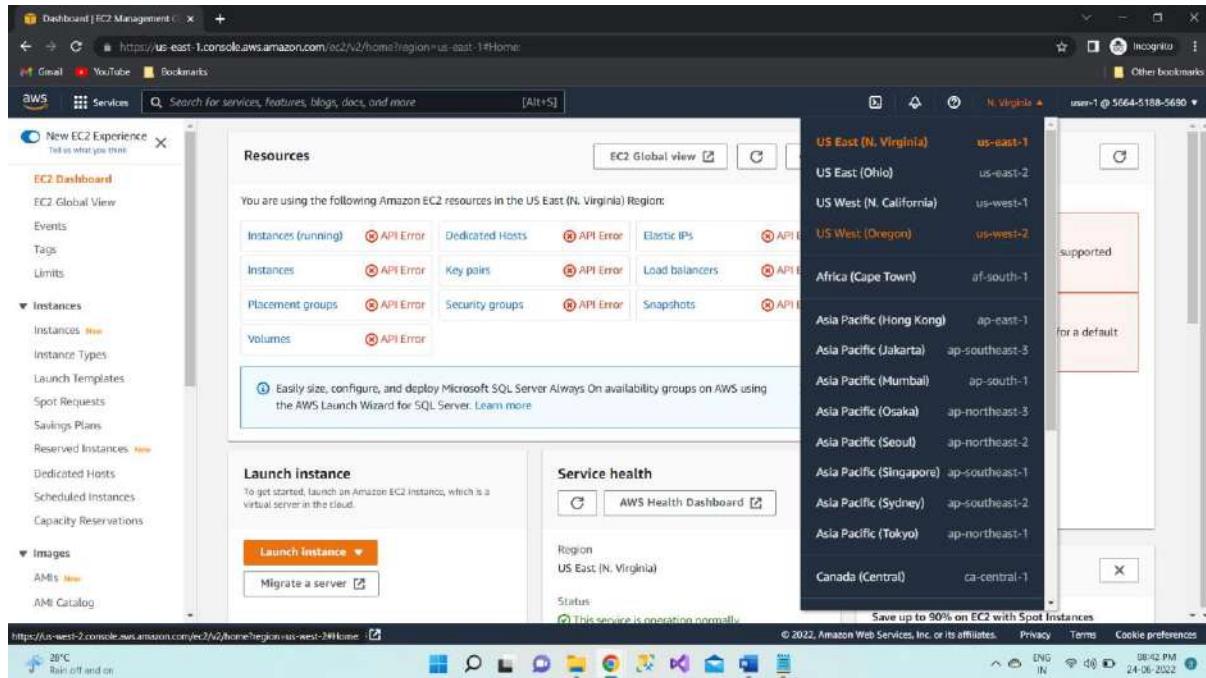
28°C Rain off and on

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 08:49 PM 24-06-2022

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: 120110b1badd1850ee85f6a5e8fb0uf6521ed77fb5a5779d5a54cdd048b	Read	Read, Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	-	-
Authenticated users group (anyone with an AWS account) Group: http://acs.amazonaws.com/groups/global/AuthenticatedUsers	-	-

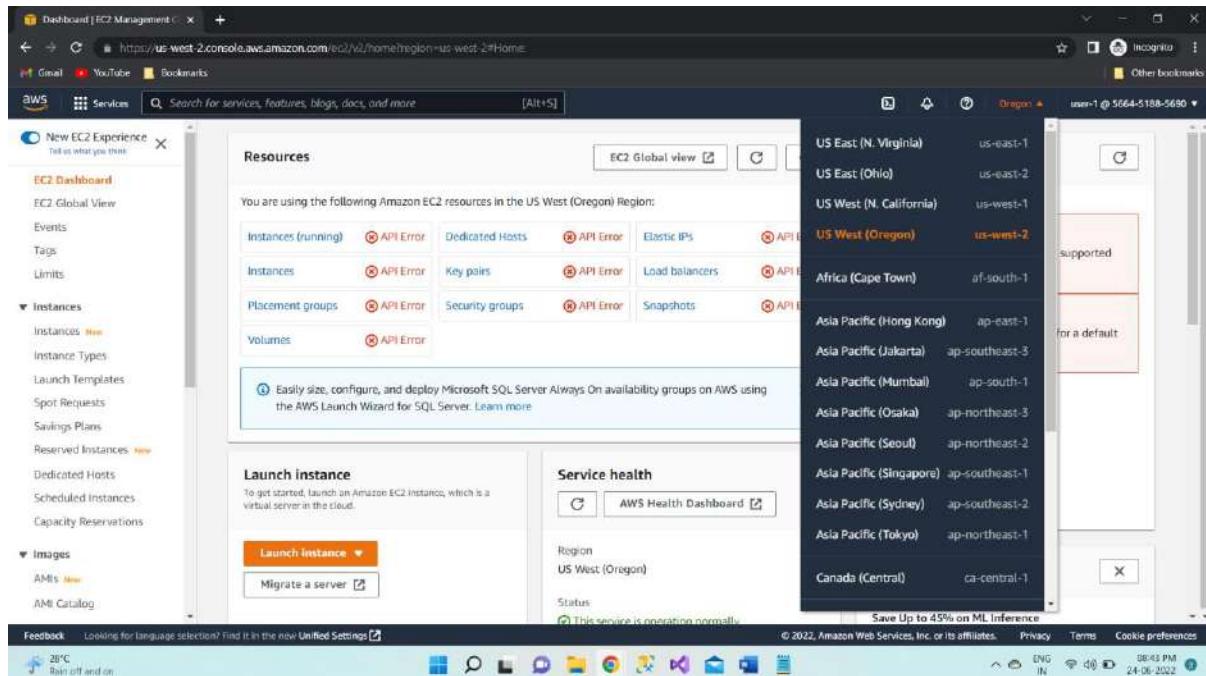
Since your user is part of the S3-Support Group in IAM, they have permission to view a list of Amazon S3 buckets and their contents. Now, test whether they have access to Amazon EC2.

**Step 37** – In the Services menu, click EC2.

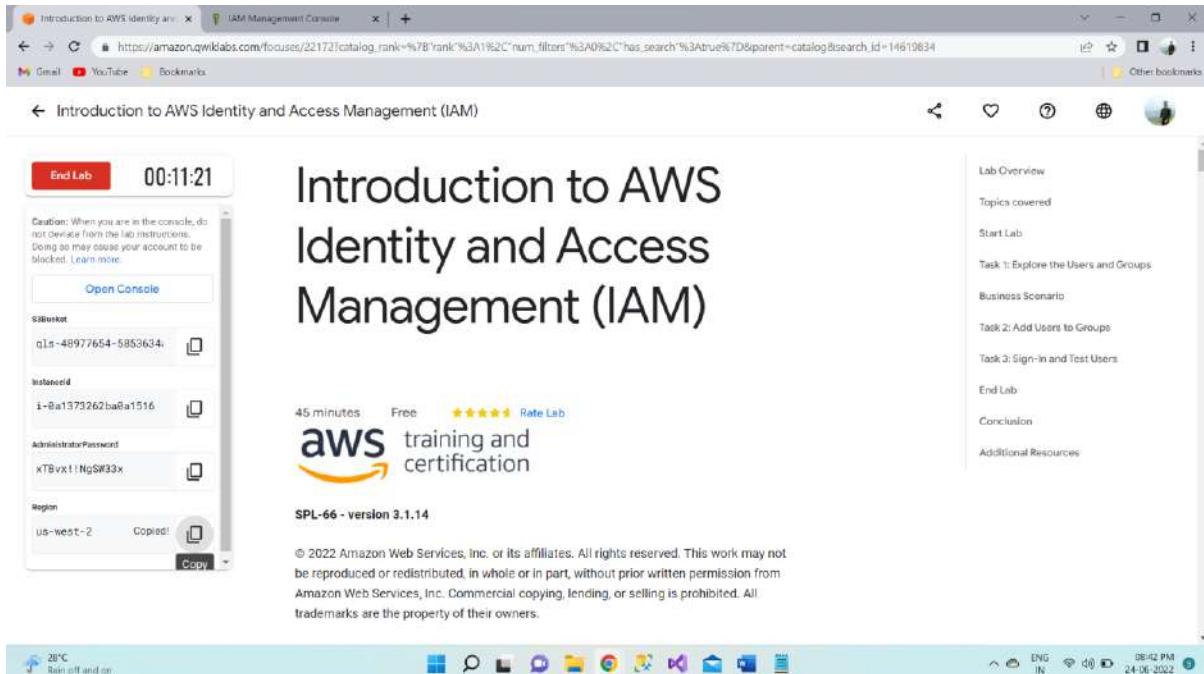


Login with new password and redo all the steps.

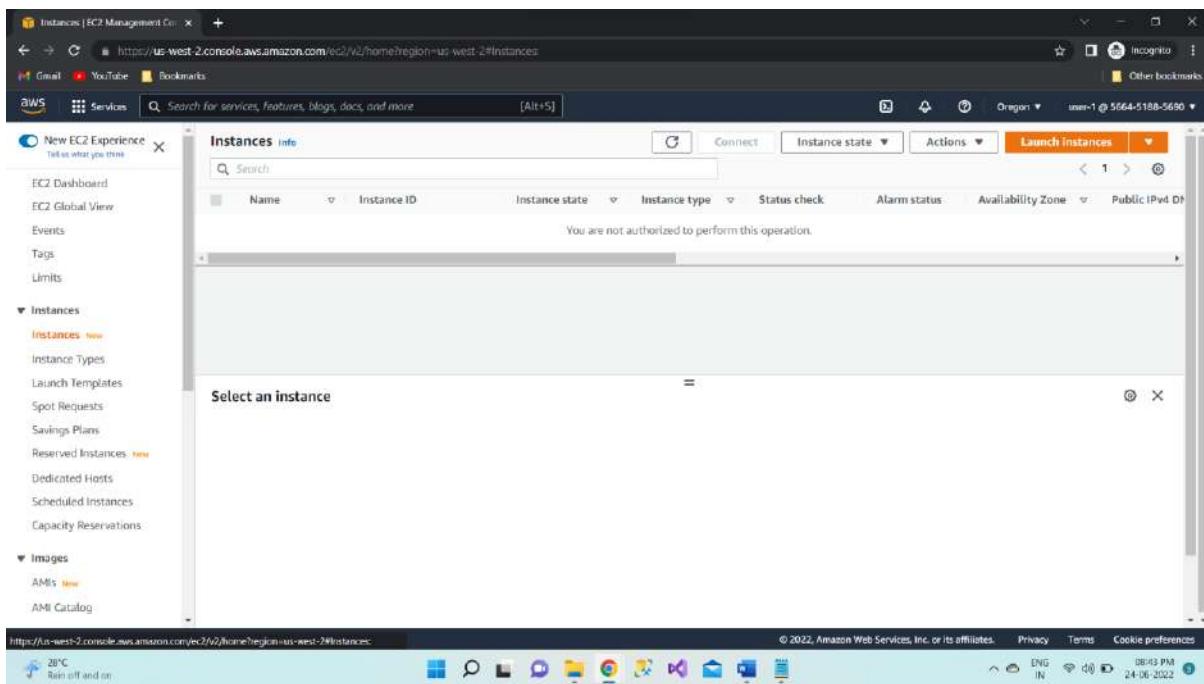
**Step 38** – Navigate to the region that your lab was launched in by: a. Clicking the drop-down arrow at the top of the screen, to the left of Support



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

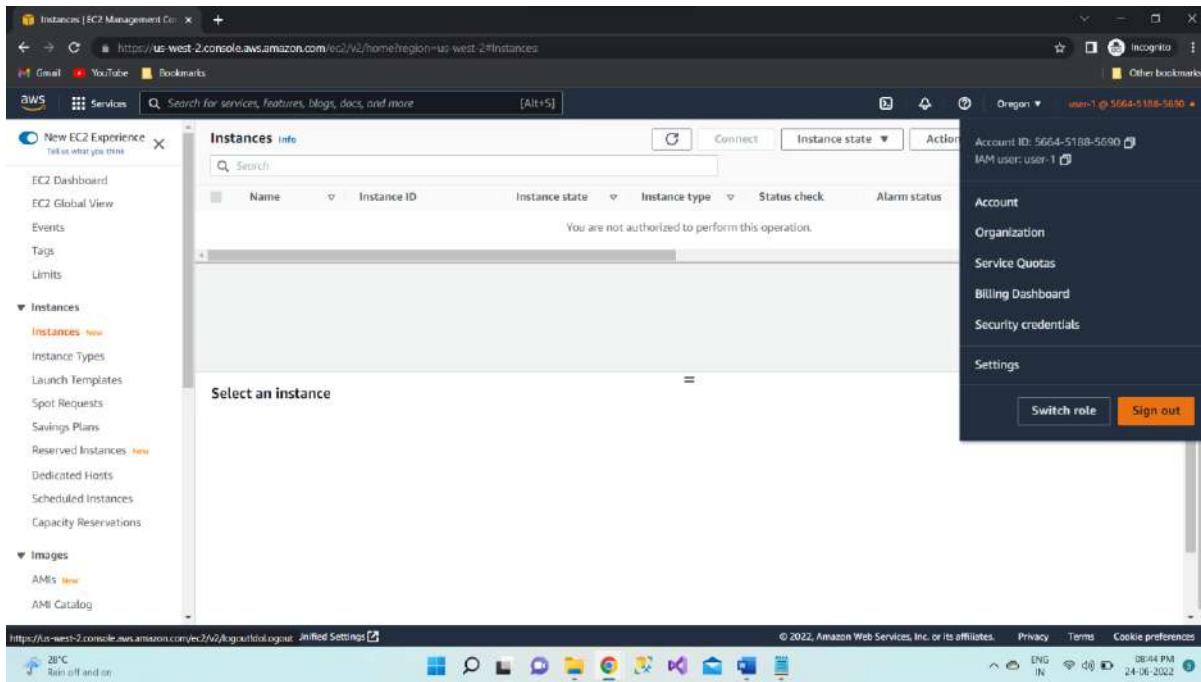


**Step 39 – In the left navigation pane, click Instances.**

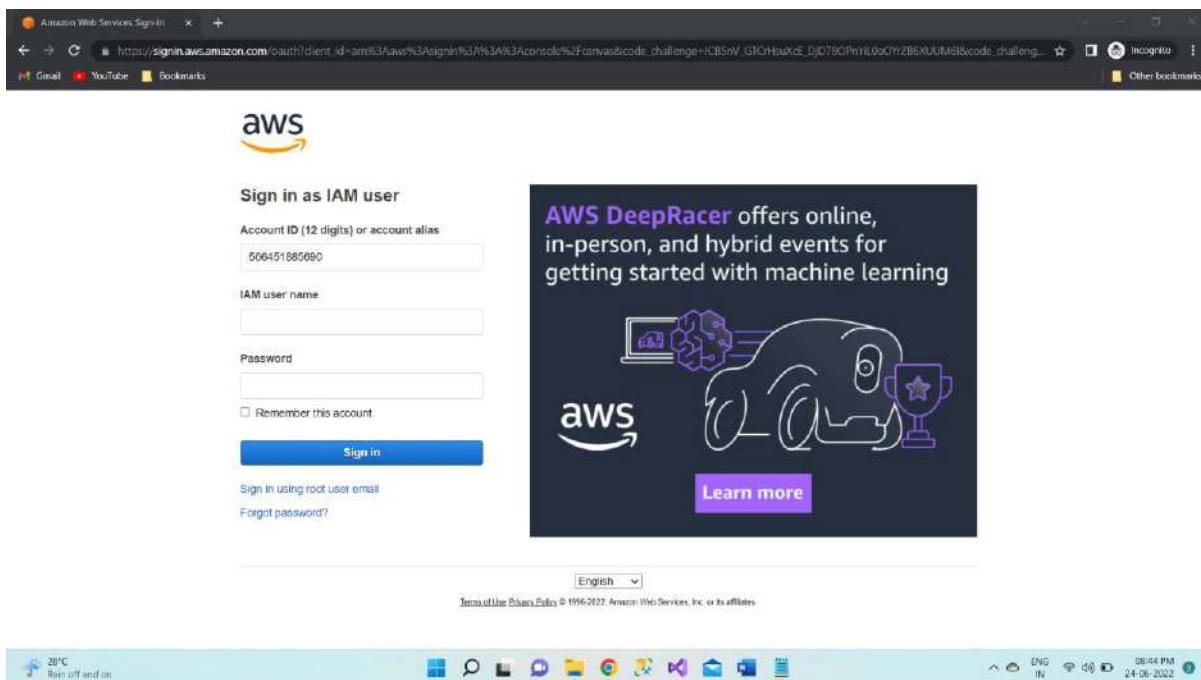


You cannot see any instances! Instead, it says an error occurred fetching instance data: You are not authorized to perform this operation... This is because your user has not been assigned any permissions to use Amazon EC2. You will now sign-in as user-2, who has been hired as your Amazon EC2 support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

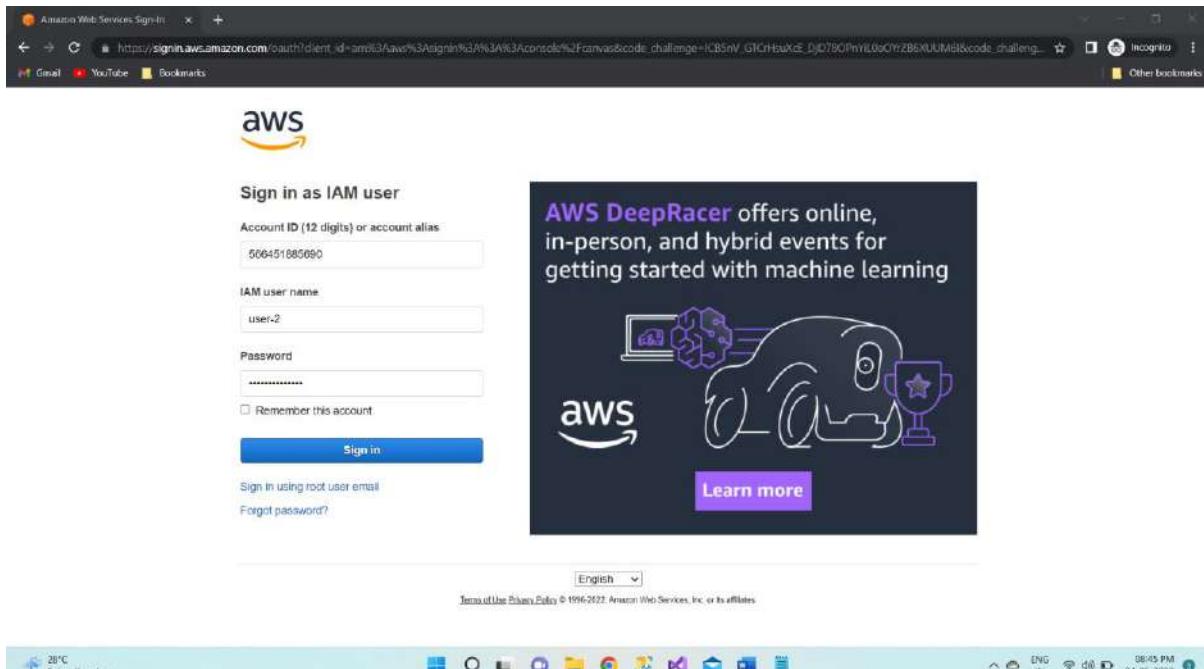
**Step 40 – Sign user-1 out of the AWS Management Console by configuring the following:** a. At the top of the screen, click user-1 b. Click Sign Out



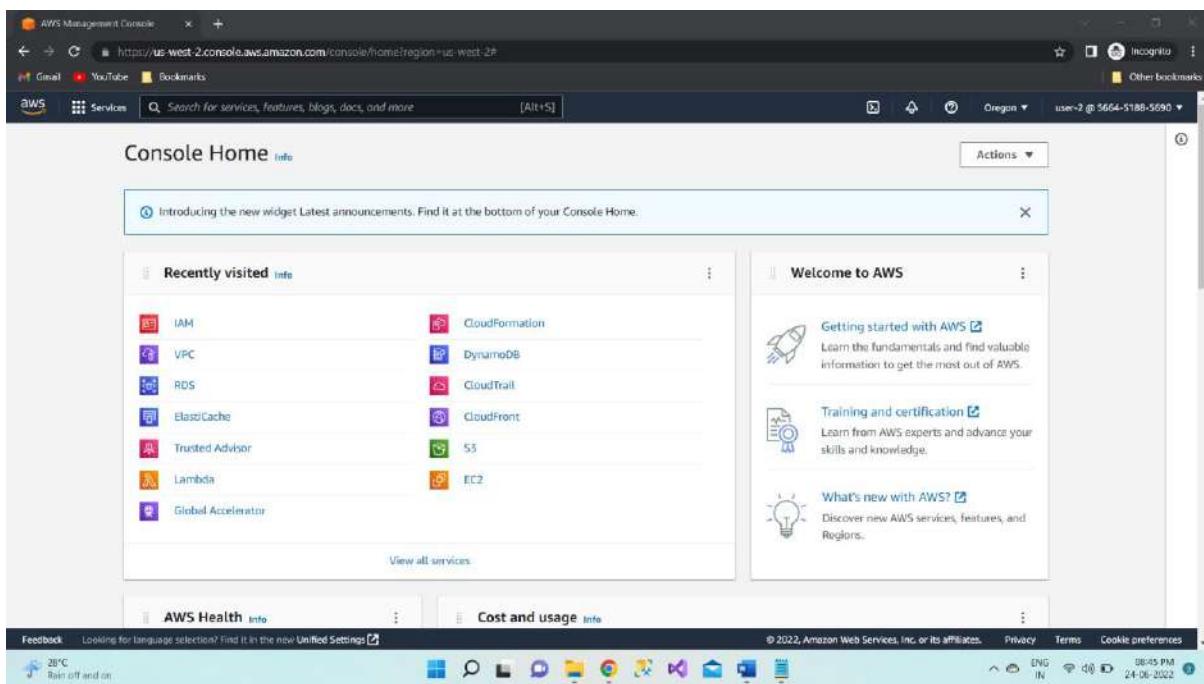
**Step 41 – Paste the IAM users sign-in link into your private window and press Enter. This links should be in your text editor.**

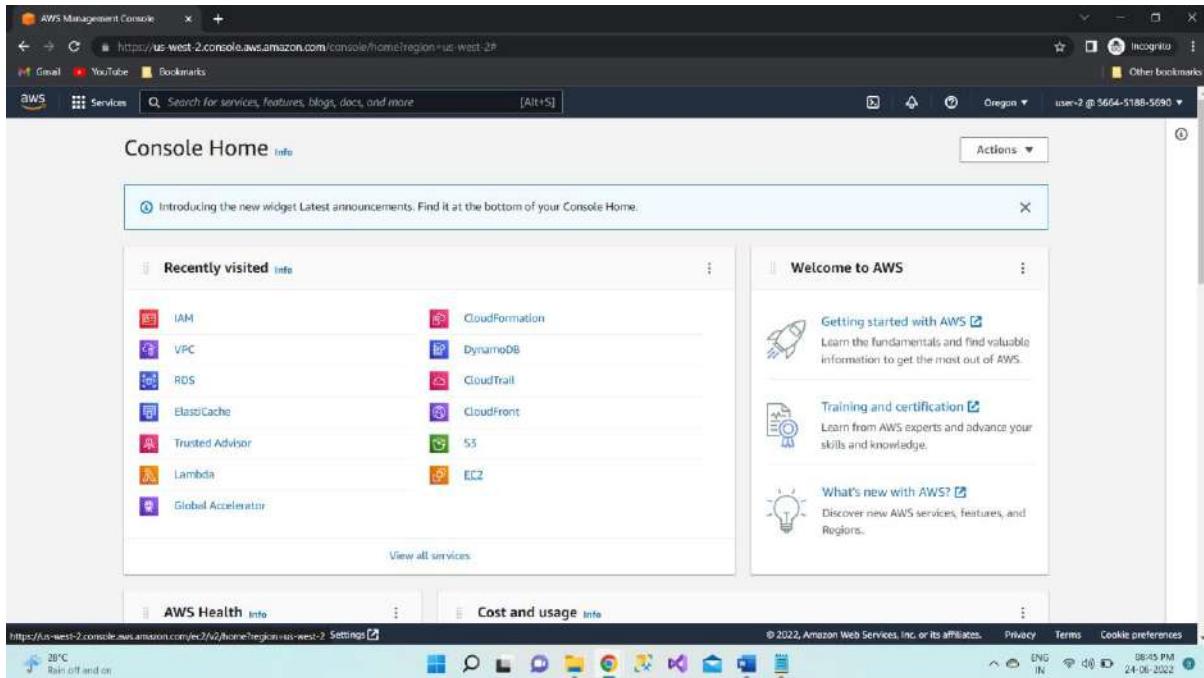


**Step 42 – Sign-in with: IAMUser name: user-2 Password: Paste the value of AdministratorPassword located to the left of these instructions.**



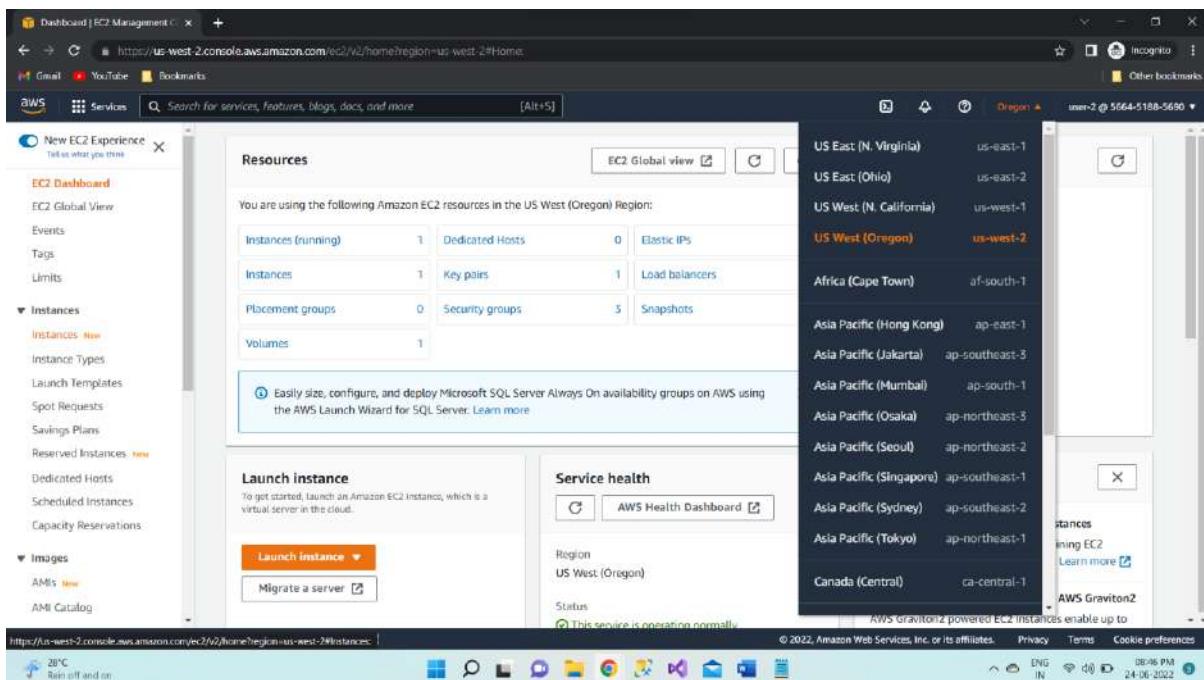
**Step 43 – In the Services menu, click EC2.**





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

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

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with sections like EC2 Dashboard, Services, Instances (selected), and Images. The main area displays a table of instances. One instance is listed: Name - i-0a1373262ba0a1516, Instance state - Running, Instance type - t3.micro, Status check - 2/2 checks passed, Alarm status - No alarms, Availability Zone - us-west-2a, Public IPv4 DNS - ec2-34-214-97-119.us-west-2.compute.amazonaws.com. Below the table, a modal window titled 'Select an instance' is open, showing the same instance details. A context menu is overlaid on the instance row, with 'Stop instance' highlighted. The bottom of the screen shows a Windows taskbar with various icons and system status.

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

The screenshot shows the AWS EC2 Management Console with the URL <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Instances>. A modal dialog box titled "Stop instance?" is displayed, asking for confirmation to stop the instance with ID i-0a1373262ba0a1516. The background shows the list of instances, including the one selected.

The screenshot shows the AWS EC2 Management Console with the same URL. A red error message box is displayed, stating: "Failed to stop the instance i-0a1373262ba0a1516. You are not authorized to perform this operation. Encoded authorization failure message: [long encoded message]". Below the message, the instance details for i-0a1373262ba0a1516 are shown, including its public IPv4 address (34.214.97.119), instance state (Running), and private IP DNS name (ip-10-1-11-109.us-west-2.compute.internal).

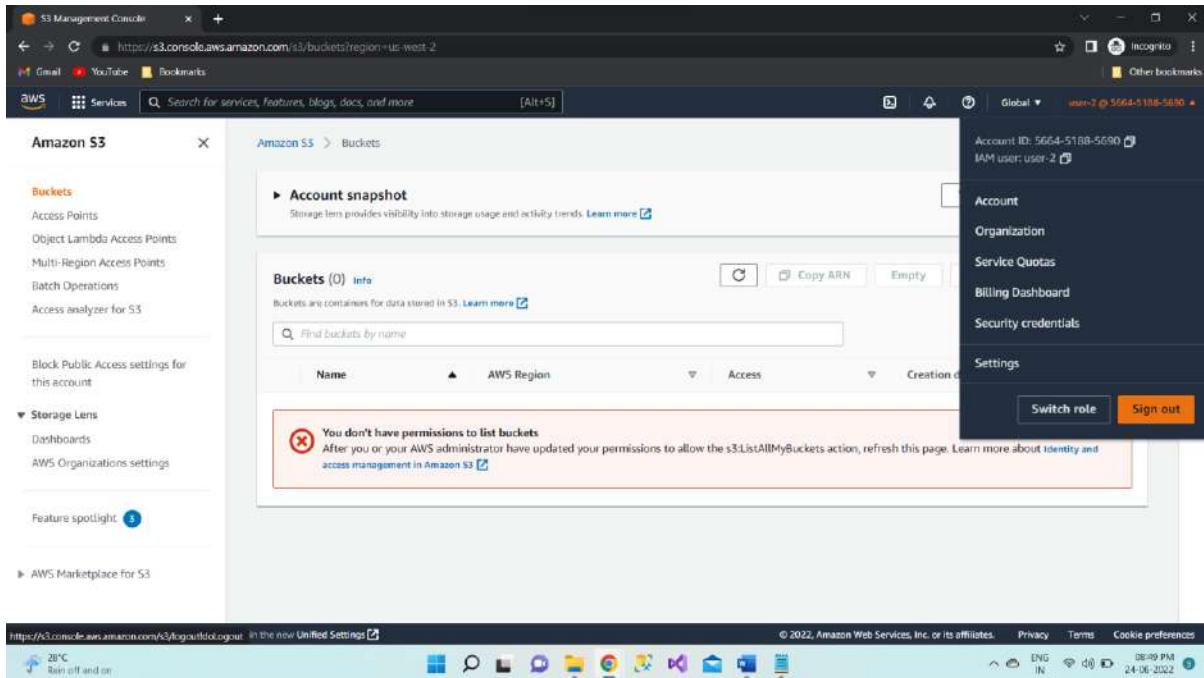
You will receive an error stating You are not authorized to perform this operation. This demonstrates that the policy only allows you to information, without making changes.

**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.

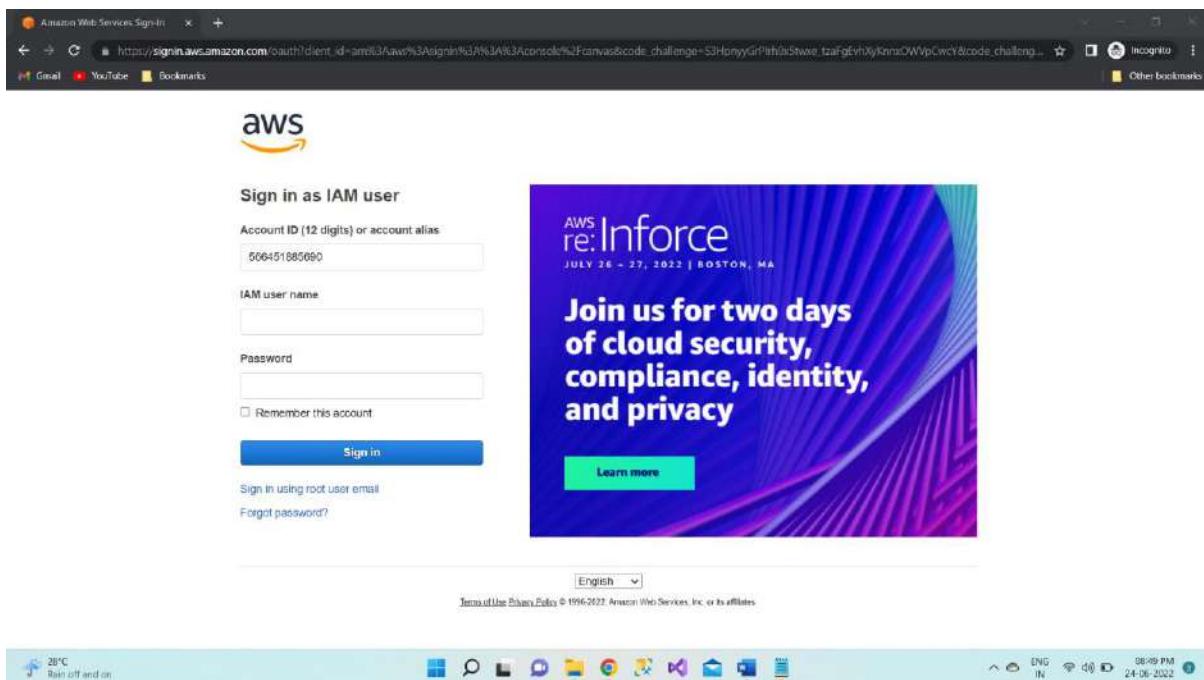


**Step 50** – Paste the IAM users sign-in link into your private window and press Enter.

**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:

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

The screenshot shows a web browser window with two main sections. On the left is the 'Amazon Web Services Sign-In' page, which displays a 'Sign in as IAM user' form. The form includes fields for 'Account ID (12 digits) or account alias' (566451885690), 'IAM user name' (user-3), 'Password', and a 'Remember this account' checkbox. Below the form is a blue 'Sign in' button. At the bottom of the sign-in section are links for 'Sign in using root user email!' and 'Forgot password?'. To the right of the sign-in form is a promotional banner for the 're:Inforce' event, held on JULY 26 - 27, 2022, in BOSTON, MA. The banner features a purple and blue abstract background and the text: 'Join us for two days of cloud security, compliance, identity, and privacy'. A 'Learn more' button is at the bottom of the banner.

The browser's address bar shows the URL: [https://signin.aws.amazon.com/oauth?client\\_id=amzn1%3wave%3A1signIn%3A%3Aconsole%3Fcanvas&code\\_challenge=53HonyGrPih%3Shwe\\_tzaifgfvh%3YknmOWVpCwct&code\\_challeng...](https://signin.aws.amazon.com/oauth?client_id=amzn1%3wave%3A1signIn%3A%3Aconsole%3Fcanvas&code_challenge=53HonyGrPih%3Shwe_tzaifgfvh%3YknmOWVpCwct&code_challeng...)

The screenshot shows the 'AWS Management Console' home page for the 'us-west-2' region. The top navigation bar includes the AWS logo, a search bar, and a 'Services' dropdown. The main content area is titled 'Console Home' and features several sections: 'Recently visited' (CloudFront, CloudTrail, DynamoDB, CloudFormation, Global Accelerator, Lambda, Trusted Advisor, ElastiCache, RDS, VPC, IAM, EC2, S3), 'Welcome to AWS' (Getting started with AWS, Training and certification, What's new with AWS), 'AWS Health' (status), and 'Cost and usage' (cost summary). The browser's address bar shows the URL: <https://us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2>. The status bar at the bottom indicates the date as 24-06-2022 and the time as 08:57 PM.

**Resources**

You are using the following Amazon EC2 resources in the US West (Oregon) Region:

Instances (running)	Instances	Placement groups	Volumes	EC2 Global view
Dedicated Hosts	Key pairs	Security groups	Snapshots	C
Elastic IPs	Load balancers	API Error	API Error	⋮

**Account attributes**

**Supported platforms**

- An error occurred: An error occurred retrieving supported platforms.
- An error occurred: An error occurred checking for a default VPC.

**Service health**

Region: US West (Oregon)

**Explore AWS**

**Instances (1) Info**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
-	i-0a1573262ba0a1516	Running	t3.micro	2/2 checks passed	No alarms	us-west-2a	ec2-34-214-9

**Select an instance**

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

The screenshot shows the AWS EC2 Management Console interface. On the left, a sidebar navigation bar includes links for EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, and Images (AMIs, AMI Catalog).

The main content area displays the 'Instances (1)' page. It lists a single instance:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
-	i-0a1373262ba0a1516	Running	t3.micro	2/2 checks passed	No alarms	us-west-2a	ec2-34-214-97-119.us-west-2.compute.amazonaws.com

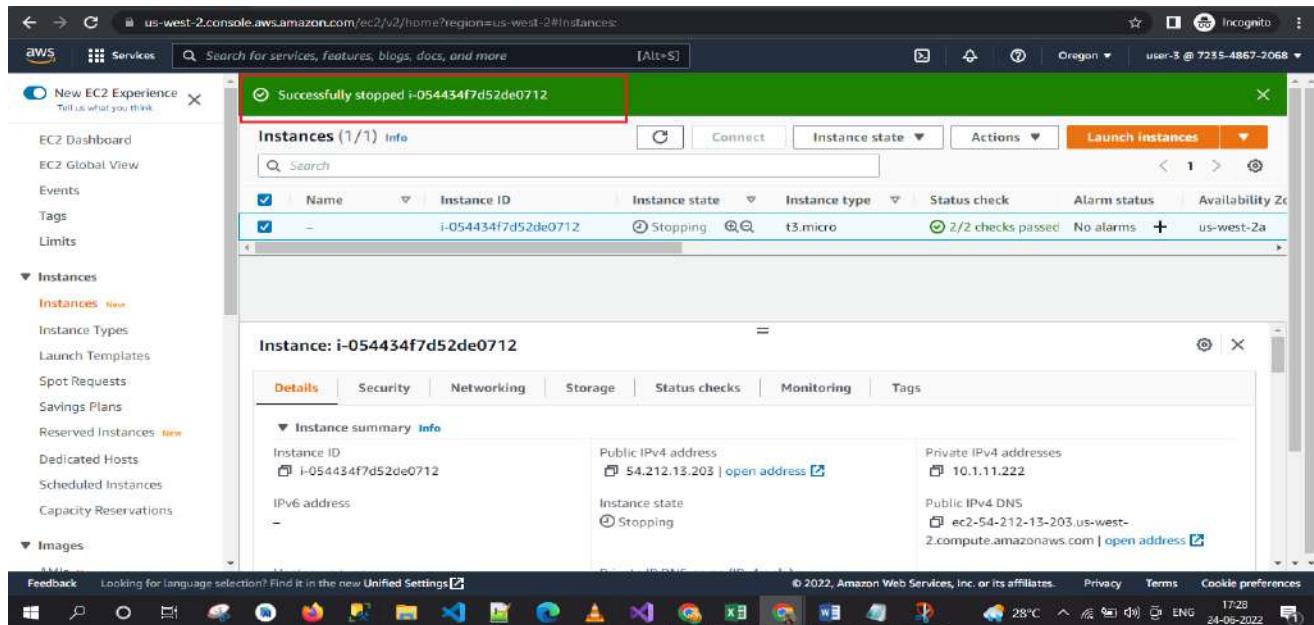
An 'Actions' dropdown menu is open over the instance row, showing options like Stop instance, Start instance, Reboot instance, Hibernate instance, Terminate instance, Instance settings (Networking, Security, Image and templates, Monitor and troubleshoot), and Hostname type (IP name, IP address). The 'Stop instance' option is highlighted.

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

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with options like EC2 Dashboard, Events, Tags, Limits, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations, and Images. The main area displays a table of instances. One instance is selected, showing its details in a modal window. The instance name is 'Launch instances', ID is 'i-0a1373262ba0a1516', state is 'Running', type is 't3.micro', and it has 2/2 checks passed. It's located in 'us-west-2n' availability zone with a public IPv4 of 'ec2-34-214-97-119'. A context menu is open over this instance, with 'Stop instance' being the highlighted option. The bottom of the screen shows a taskbar with various icons and system status.

This screenshot shows a confirmation dialog box titled 'Stop instance?'. It contains the message 'To confirm that you want to stop the instance, choose the Stop button below.' Below the message, there are two buttons: 'Cancel' and 'Stop'. The 'Stop' button is highlighted with a red border. In the background, the EC2 instance list is visible, showing the same instance as the previous screenshot.



**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 – Start Lab and click on Open Console



### Step 2 – Start Lab and click on Open Console



### Step 2 – At the top-left of the AWS Management Console, on the Services menu choose S3.

The screenshot shows two side-by-side views of the AWS Management Console. The left view is the 'Old AWS Console' interface, while the right view is the 'New AWS Console Home'. A central modal window titled 'Switch now' is displayed, prompting the user to switch to the new experience.

**Old AWS Console (Left):**

- AWS services:** Recently visited services include Systems Manager, Lambda, Trusted Advisor, VPC, EC2, Elastic Container Service, IAM, S3, Elastic Kubernetes Service, CloudWatch, and RDS.
- Build a solution:** Get started with simple wizards and automated workflows.

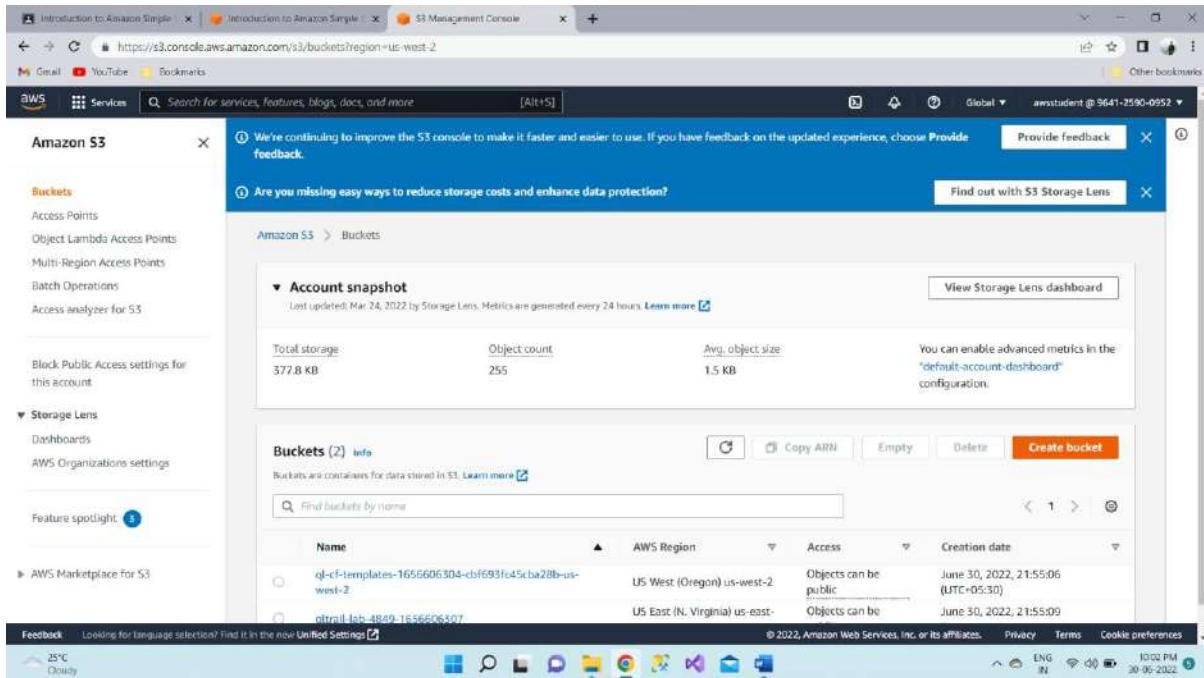
**New AWS Console Home (Right):**

- New AWS Console Home:** See valuable insights for your account and services with the new customizable Console Home experience. [Learn more](#).
- Stay connected to your AWS resources on-the-go:** AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device. [Learn more](#).

**Bottom Navigation Bar:**

- Feedback: Looking for language selection? Find it in the new Unified Settings.
- CloudWatch Metrics: 25°C, Cloudy.
- Other bookmarks: Gmail, YouTube.
- Region: Oregon.
- User: awsstudent @ 9561-2590-0952.
- Links: Privacy, Terms, Cookie preferences.
- Date and Time: 30/05/2022, 10:01 PM.

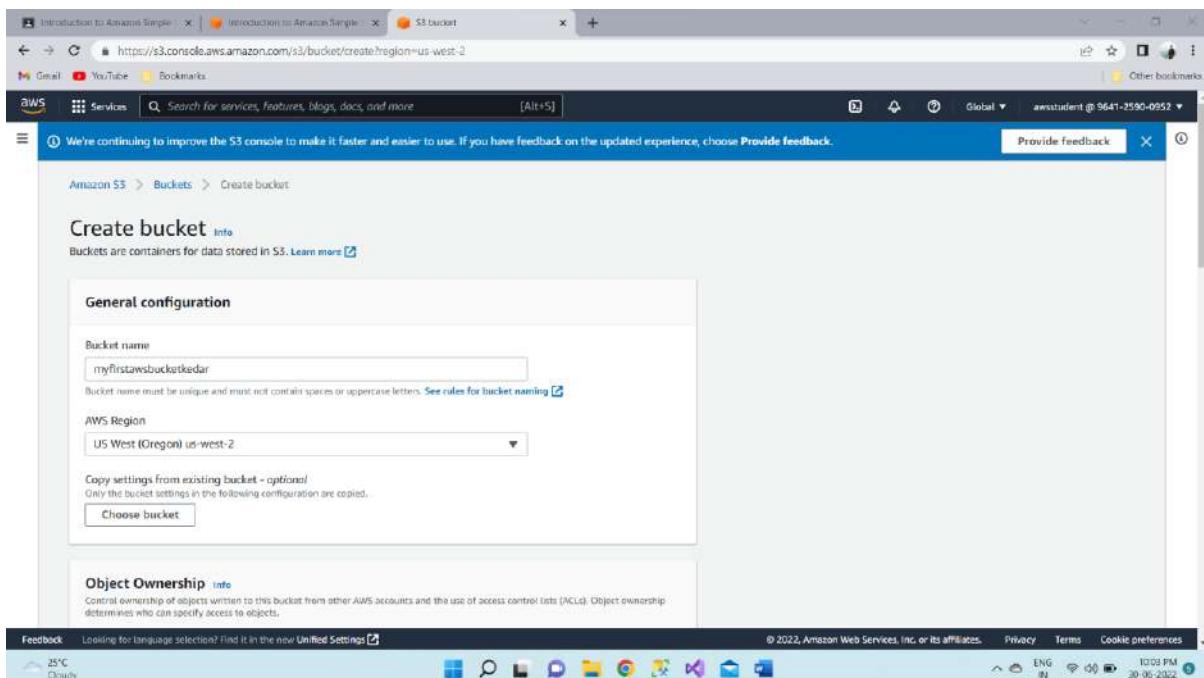
### Step 3 – Choose create bucket.



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

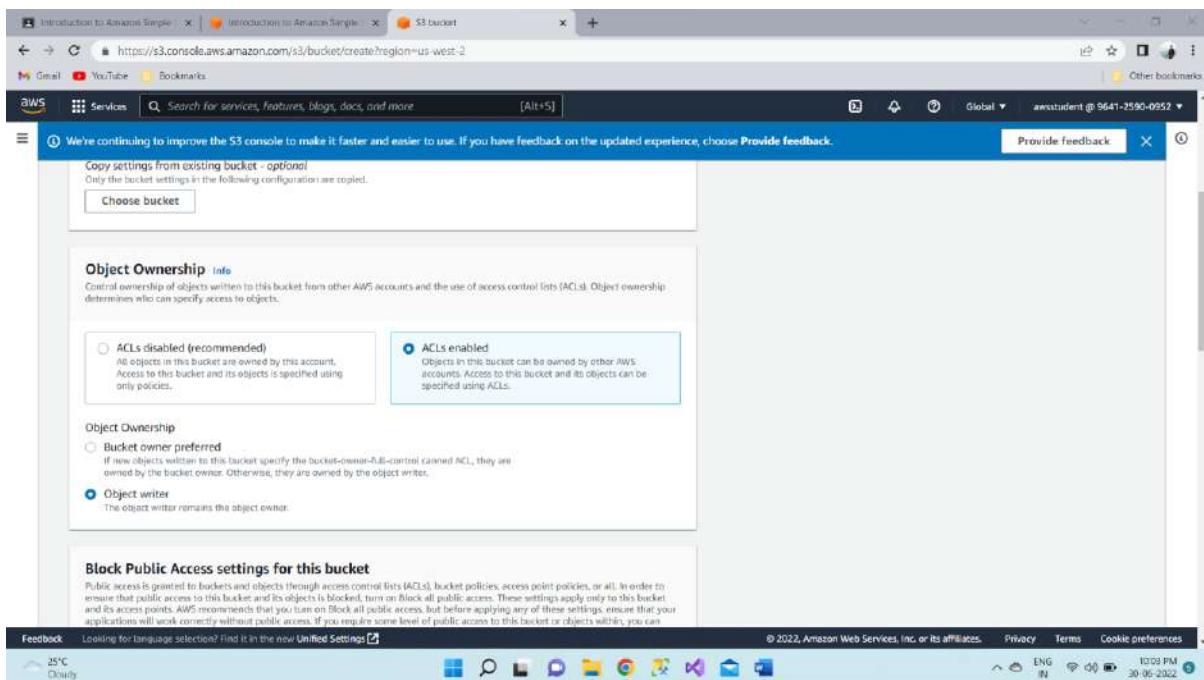
Replace in the bucket name with a random number. This ensures that you have a unique name.

\* Example Bucket Name - reportbucket987987



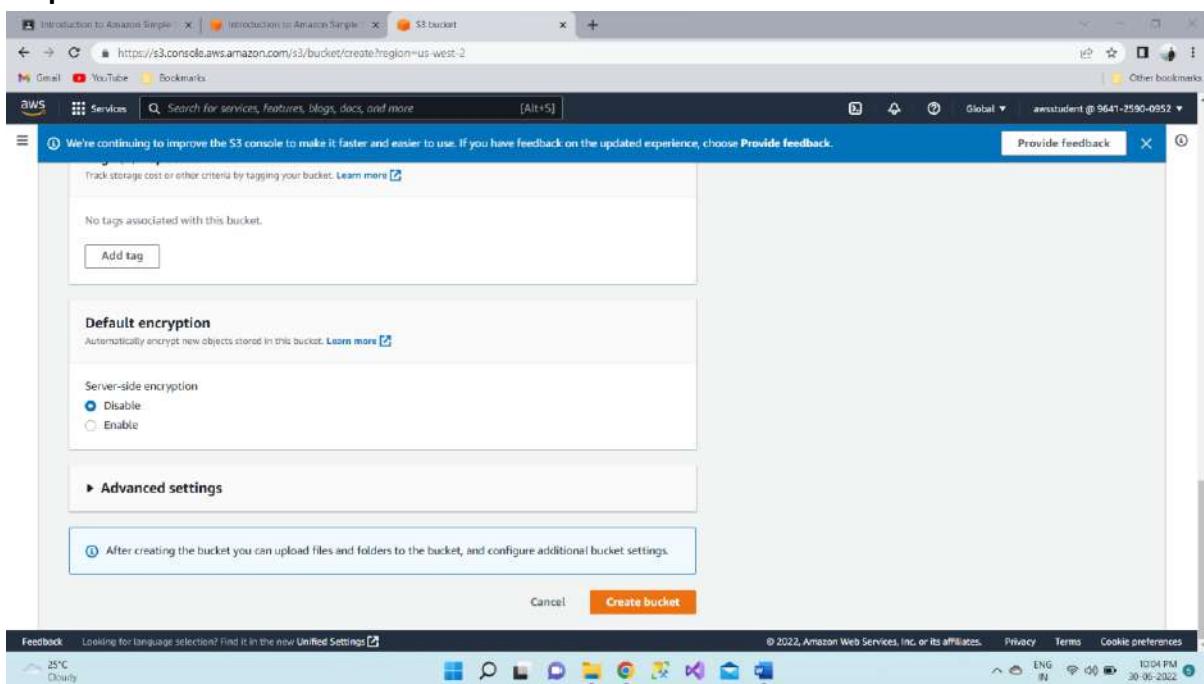
#### Step 5 – In the Object Ownership section, configure:

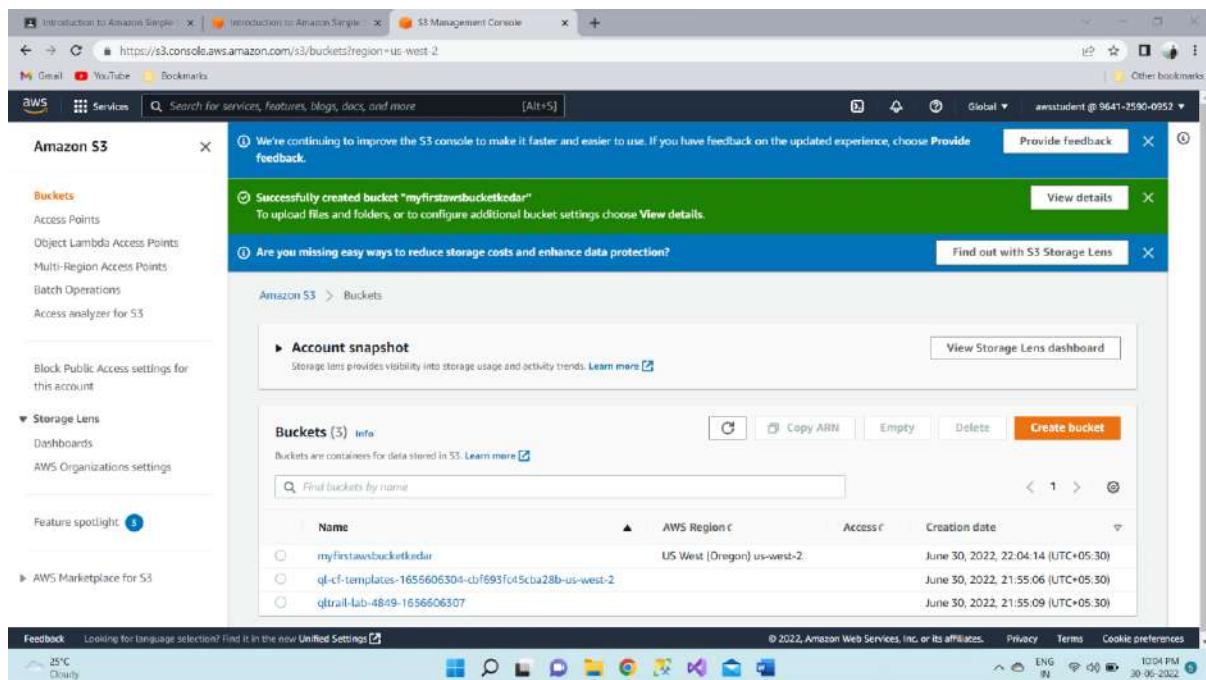
- ACLs enabled
- Object Writer



## Step 6 – Leave Region as it defaults value.

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



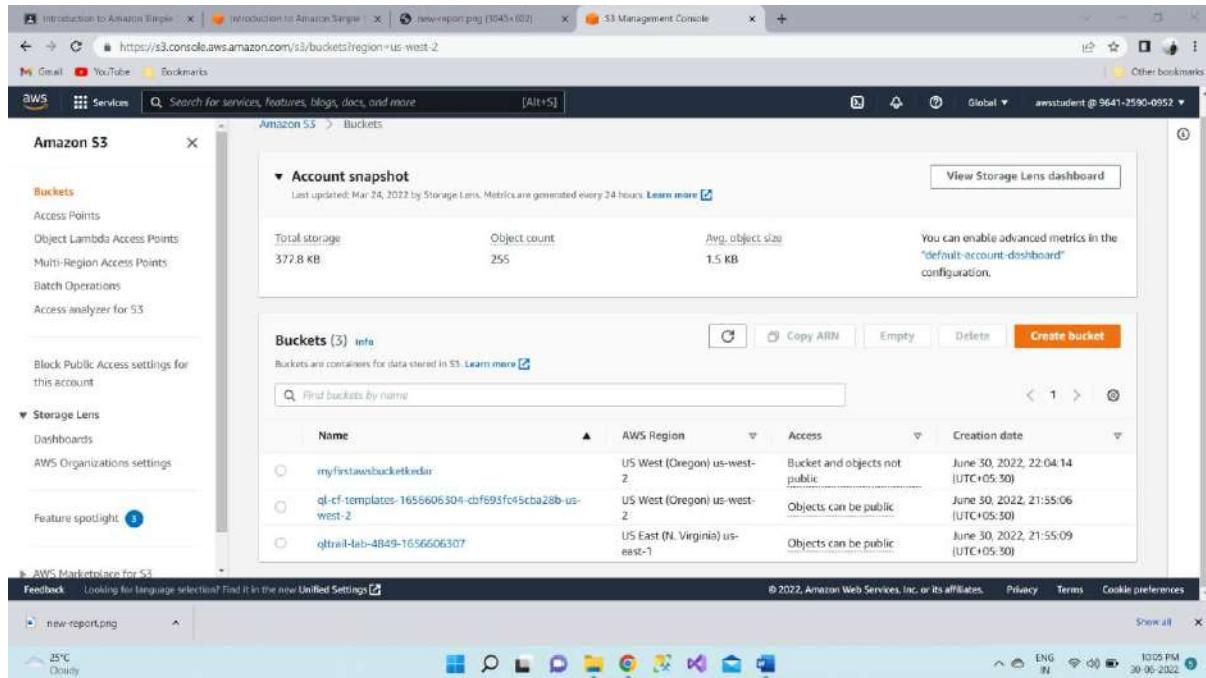


## Task 2: Upload an object to the bucket

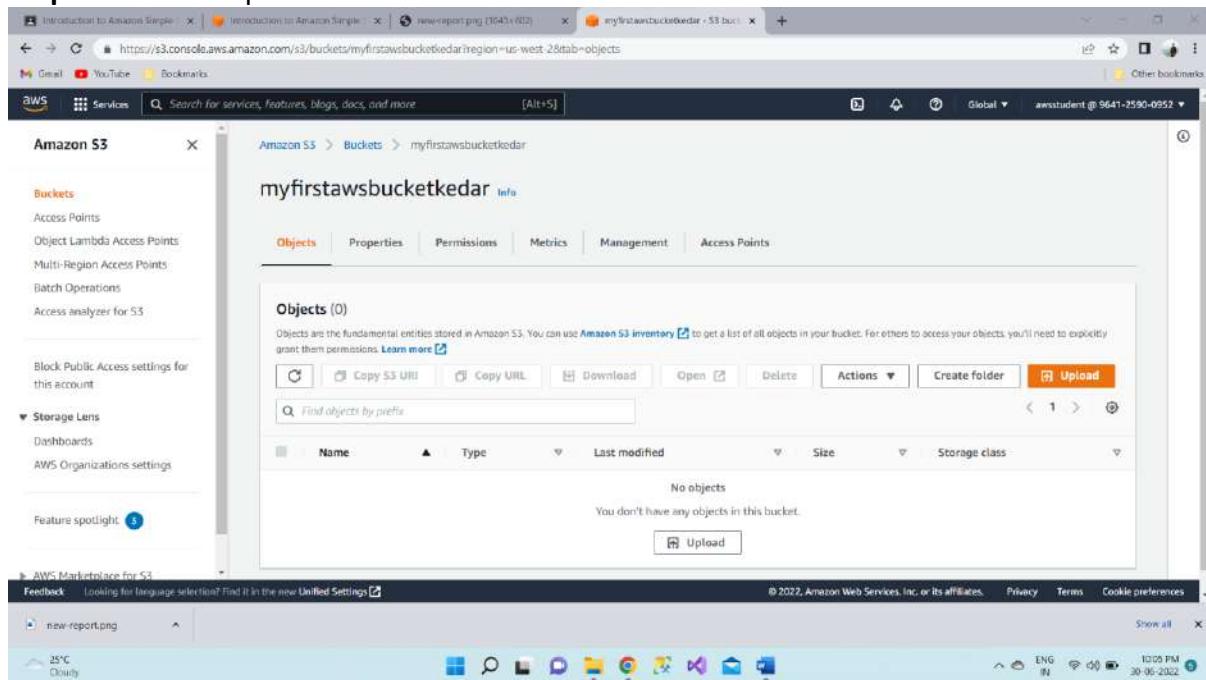
Now that you have a bucket created for your report data, you are ready to work with objects. An object can be any kind of file: a text file, a photo, a video, a zip file, and so on. When you add an object to Amazon S3, you have the option of including metadata with the object and setting permissions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

In this task you test uploading objects to your reportbucket. 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 reportbucket.**

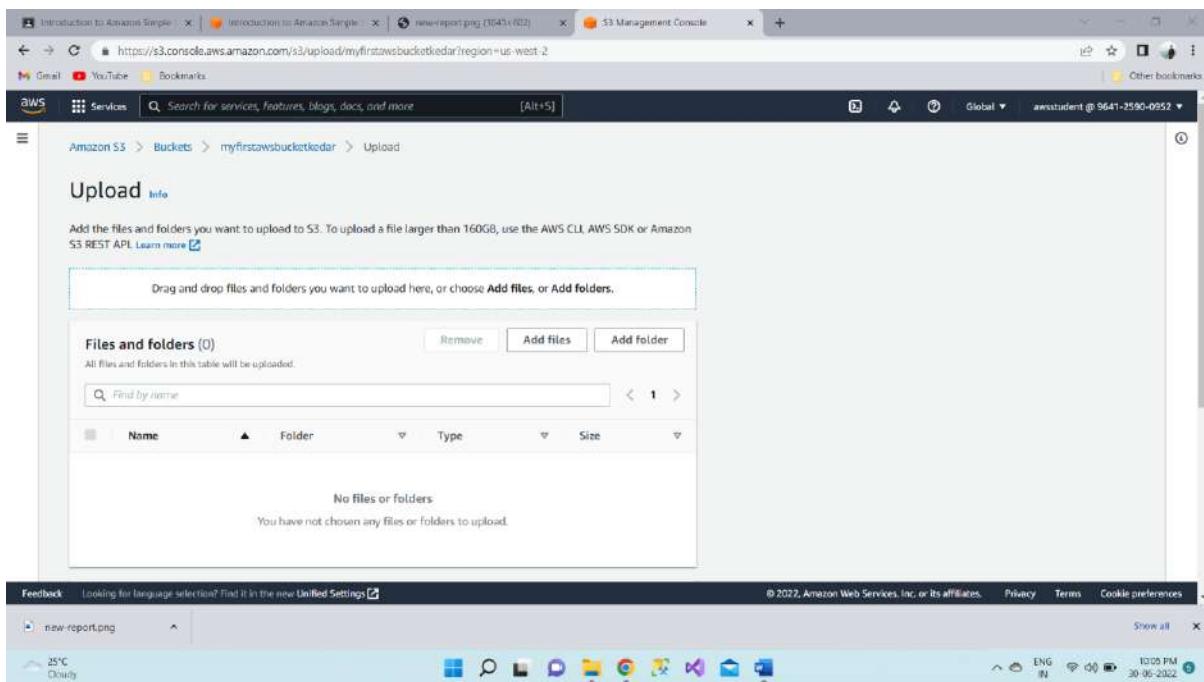


## Step 9 – Choose Upload.

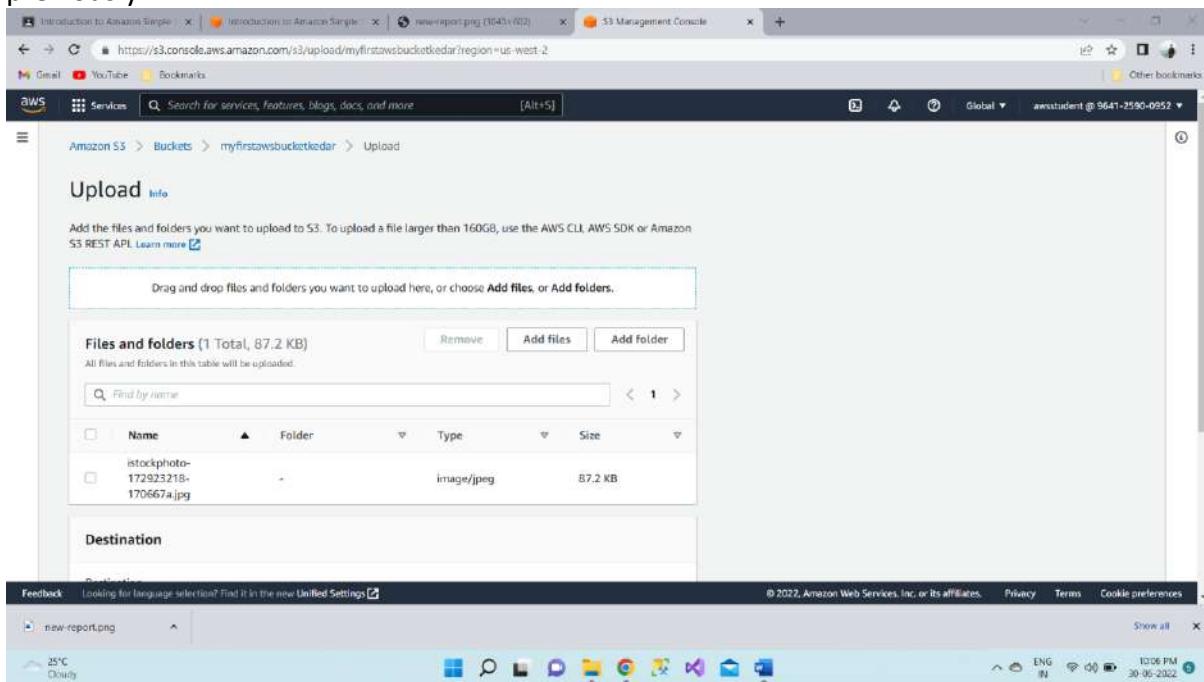


This launches an upload wizard. Use this wizard to upload files either by selecting them from a file chooser or by dragging them to the S3 window.

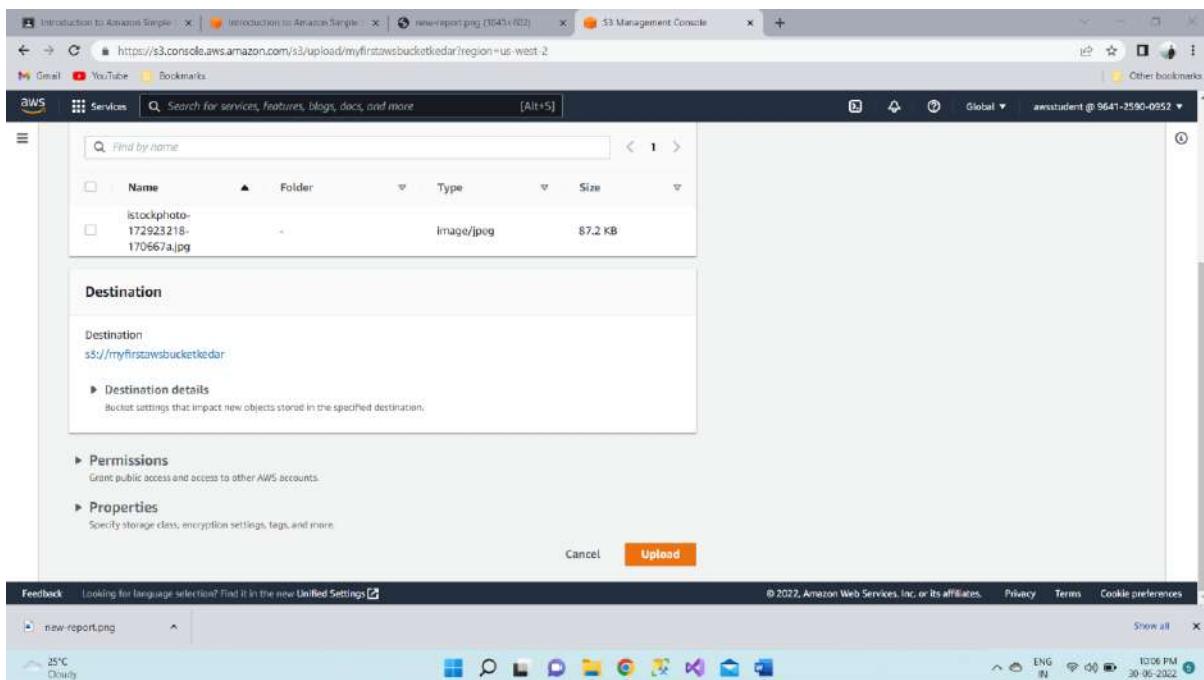
## Step 10 – Choose Add files.



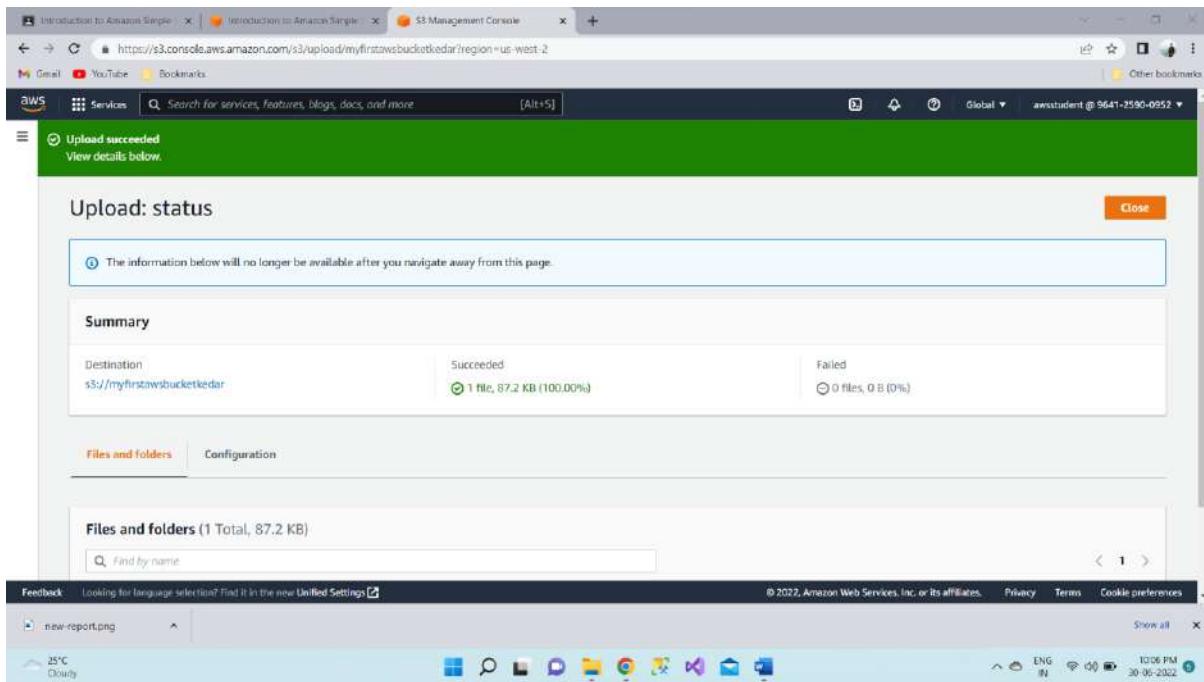
**Step 11 – Click the EC2-Support group Browse to and select the file that you downloaded previously.**



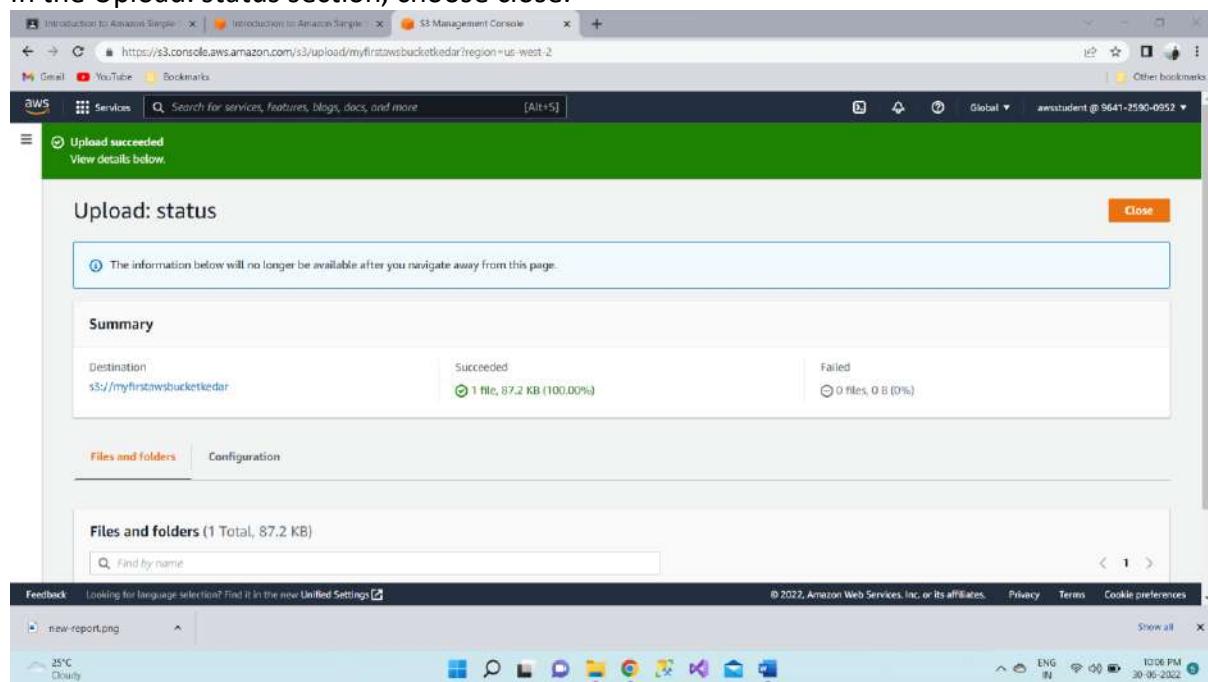
**Step 11 – Scroll down and choose Upload.**



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



In the Upload: status section, choose close.



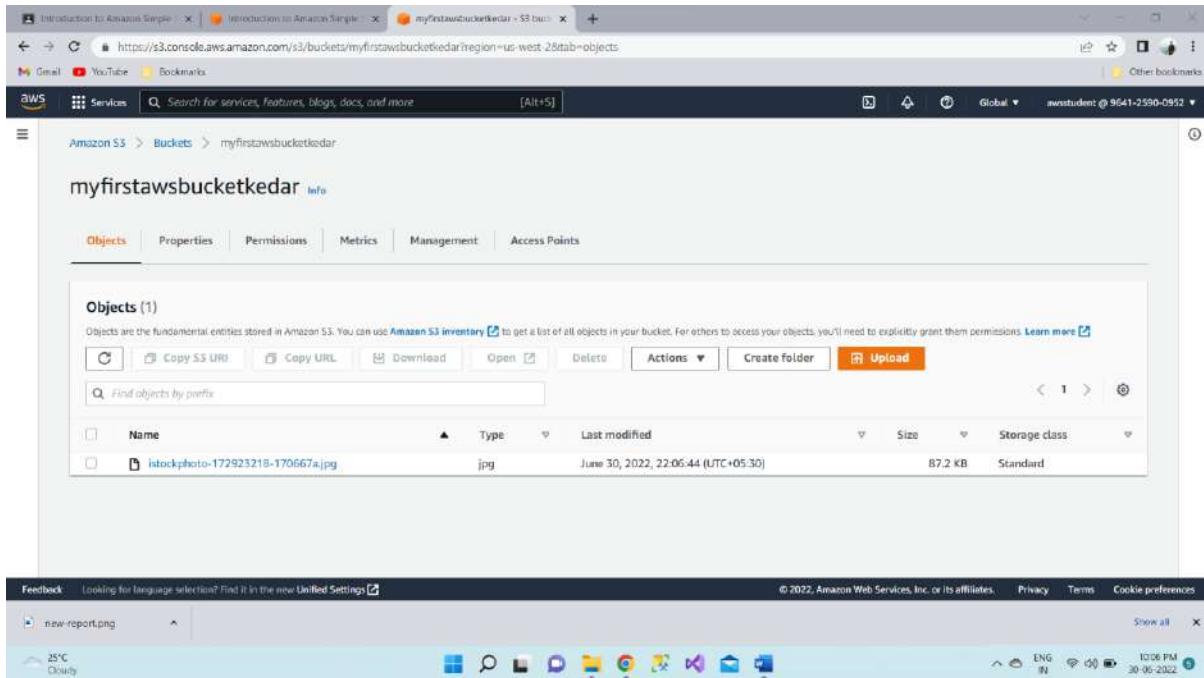
### Task 3: Make an Object public

Security is a priority in Amazon S3. Before you configure your EC2 instance to connect to the reportbucket, 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.

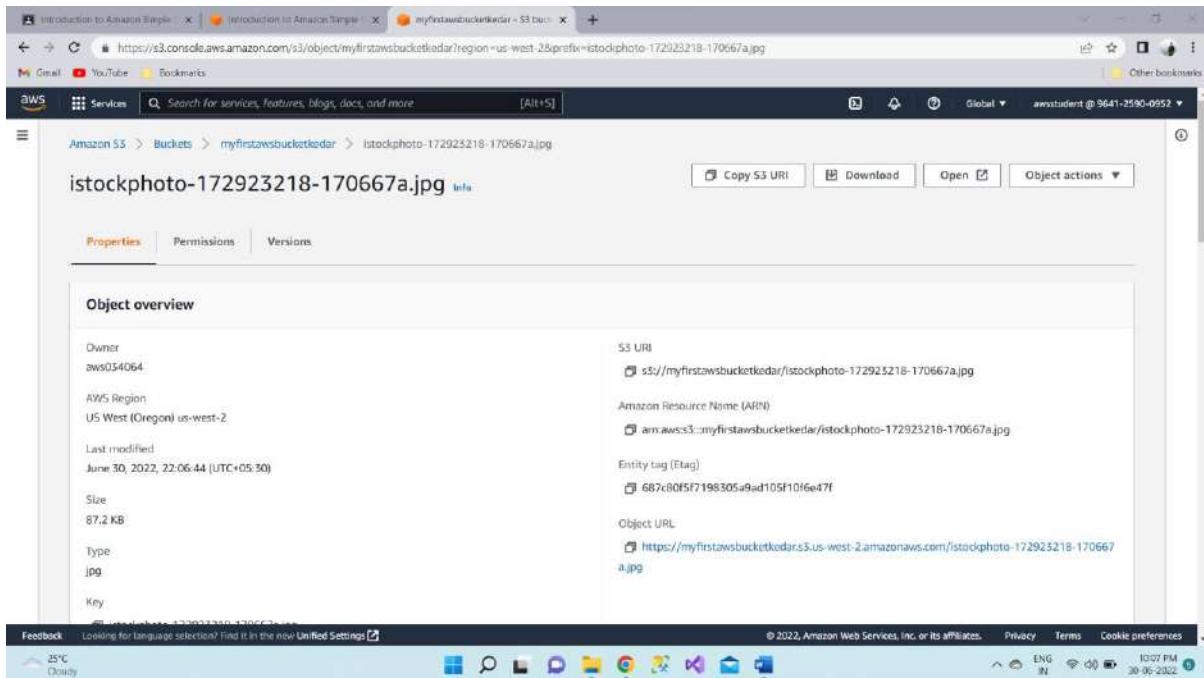
First, you attempt to access the object to confirm that it is private by default.

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



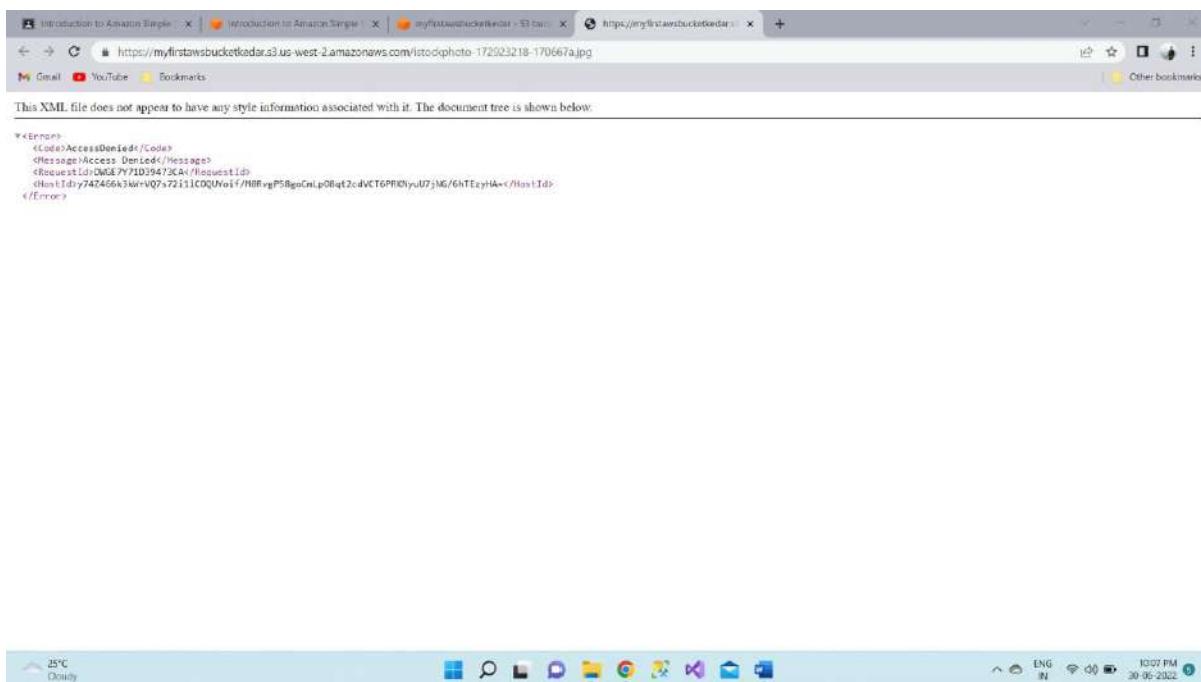
The new-report.png overview page opens. Notice that the navigation in the top-left updates with a link to return to the bucket overview page.

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



### 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.



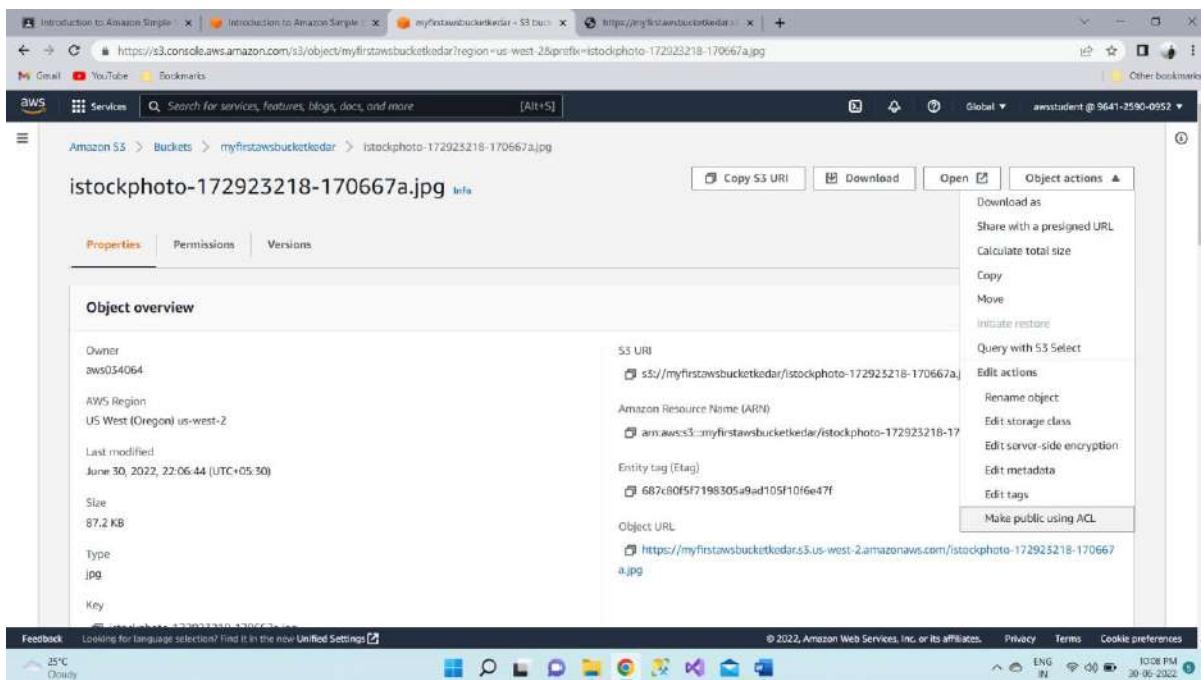
Now that you've confirmed the default security of S3 is private, you want to test how to make the object publicly accessible.

**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.

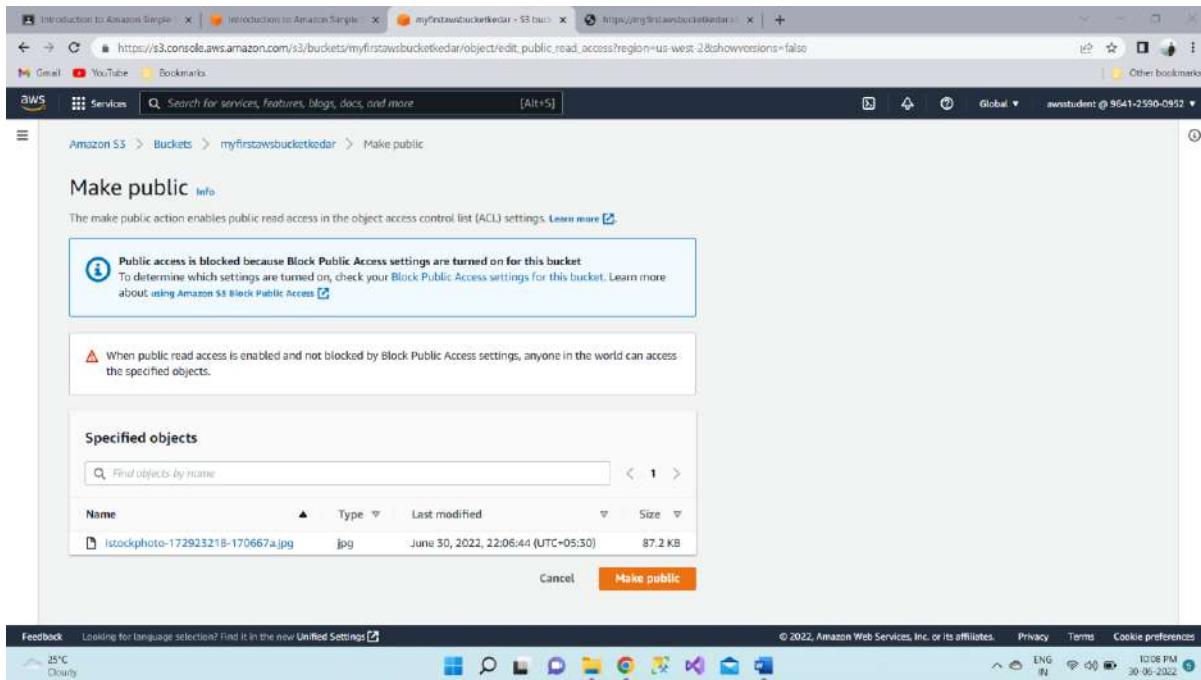
**Step 17** – Close the Show Policy window.

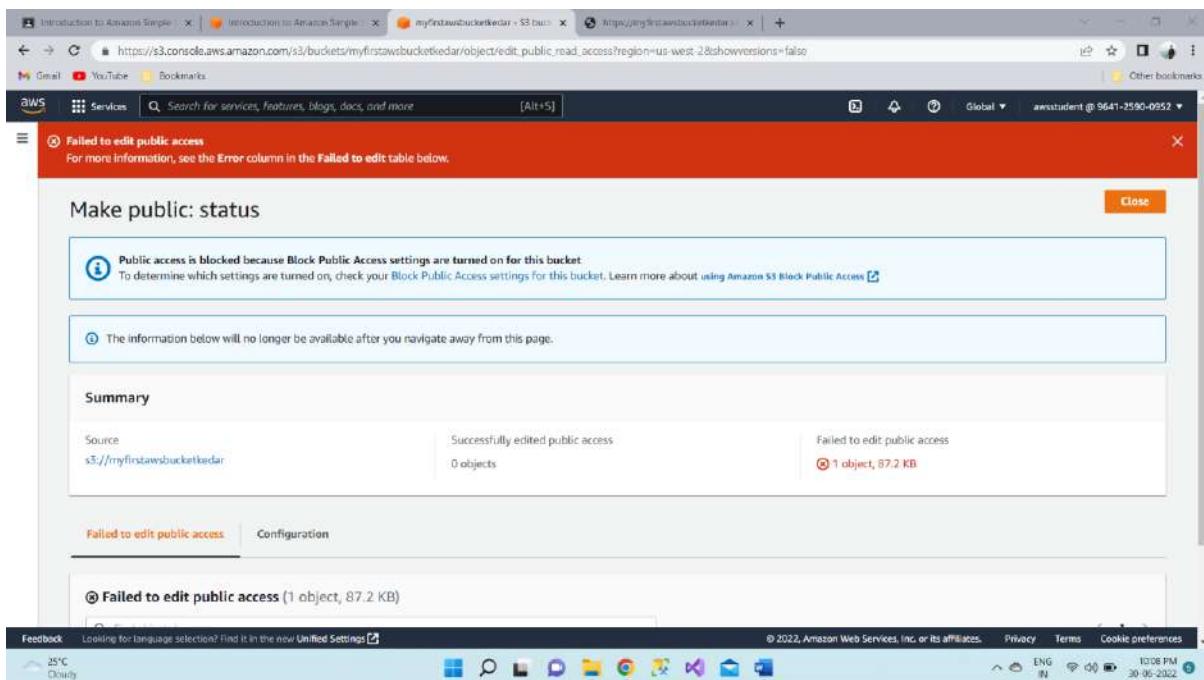
**Step 18** – Choose the Object actions button and Make public via ACL. which will be the last item in the list.



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.

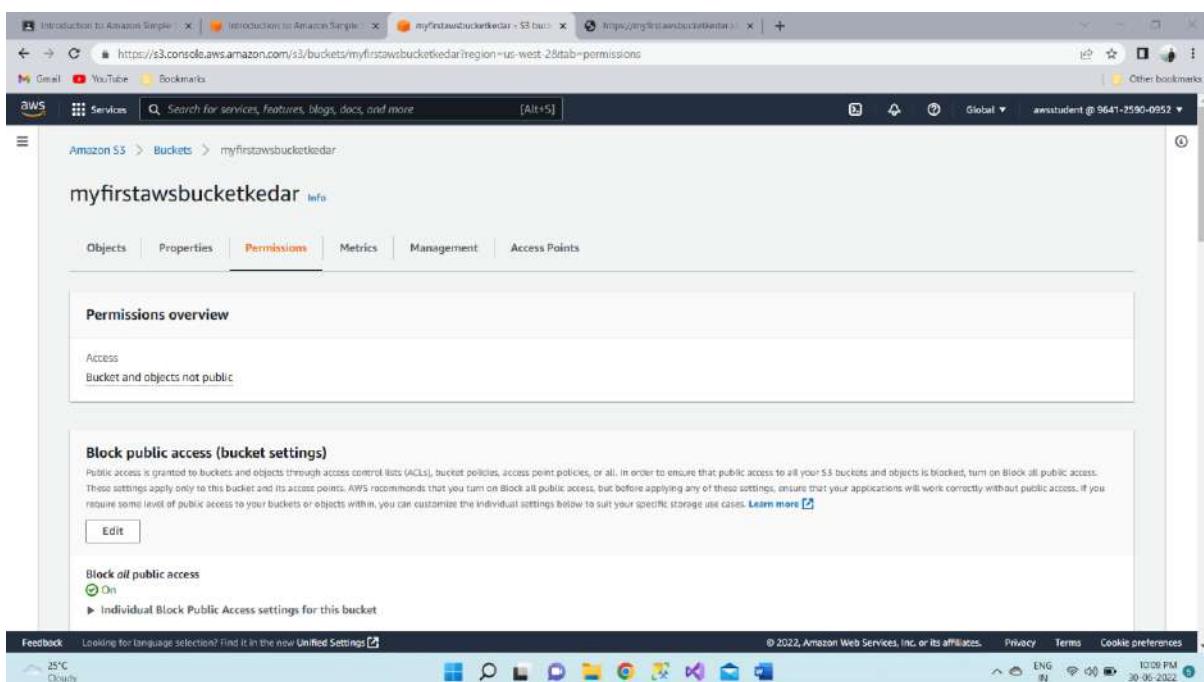




**Step 20** – Choose Close to return to the object overview.

**Step 21** – Use the navigation at the top to go back to the main reportbucket overview page.

**Step 22** – Choose Permission tab.



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

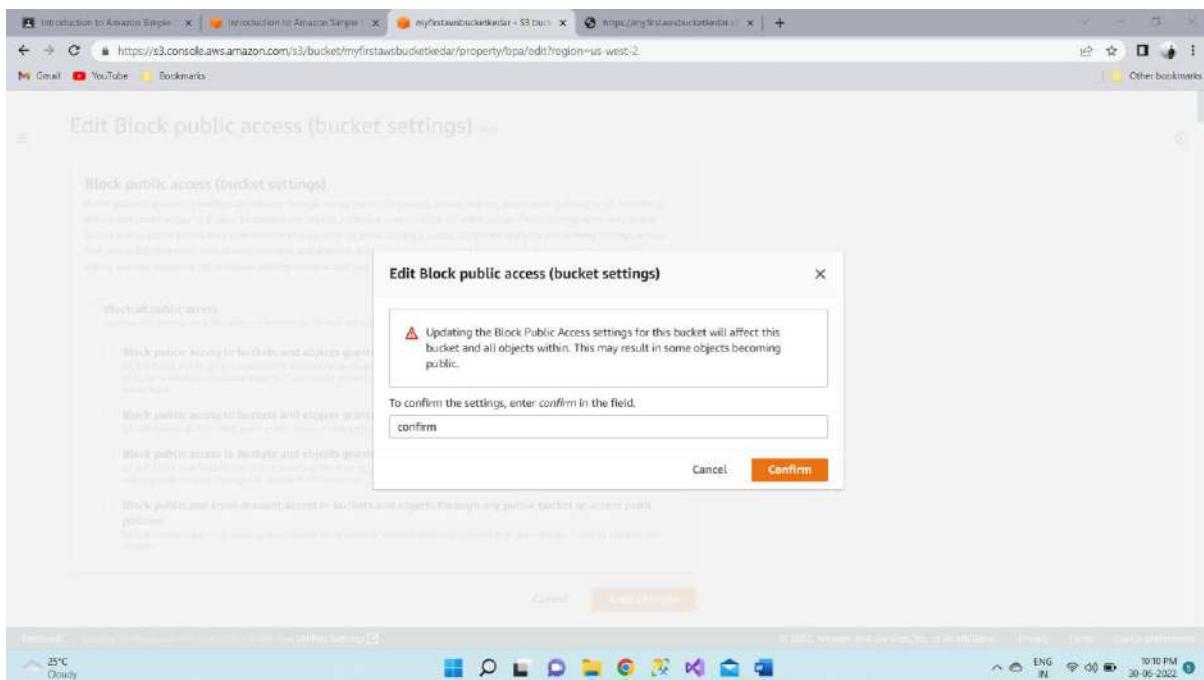
The screenshot shows the AWS S3 console with the 'myfirstawsbucketkedar' bucket selected. In the 'Permissions overview' section, under 'Block public access (bucket settings)', there is an 'Edit' button and a radio button labeled 'On' for 'Block all public access'. Below this, a note states: 'Public access is blocked because Block Public Access settings are turned on for this bucket'. The note also says: 'To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access'.

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

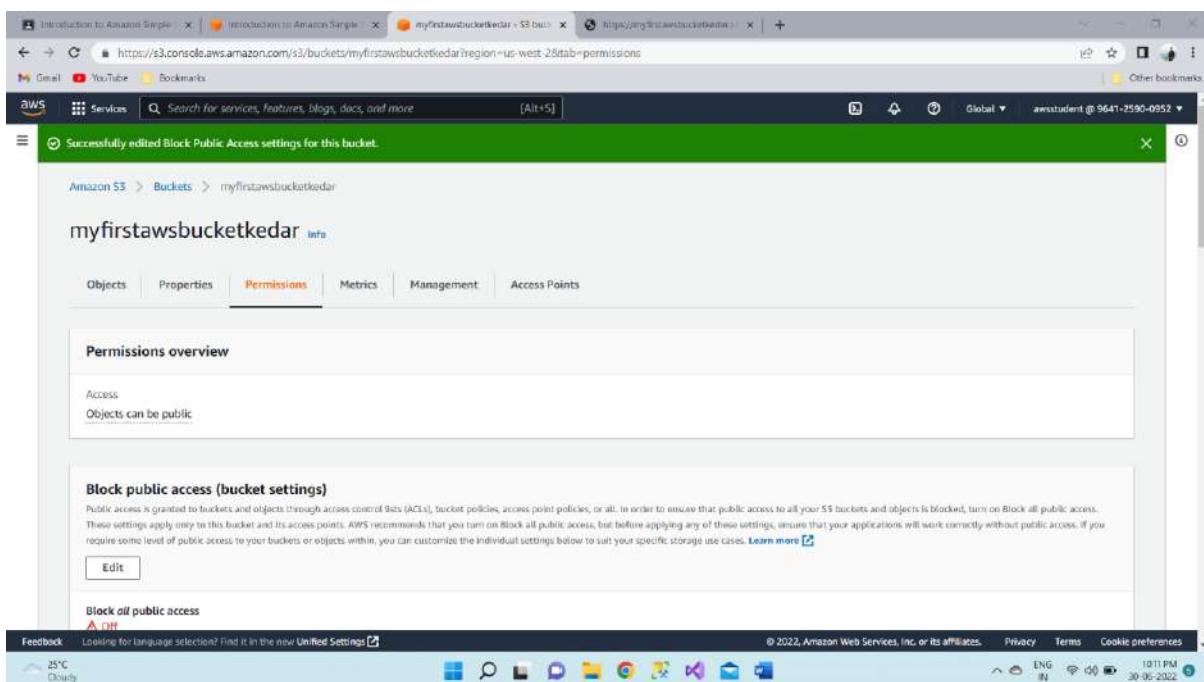
The screenshot shows the 'Edit Block public access (bucket settings)' page. The 'Block all public access' checkbox is unchecked. Below it, there are five other checkboxes under the heading 'Block public access through other settings': 'Block public access to buckets and objects granted through new access control lists (ACLs)', 'Block public access to buckets and objects granted through any access control lists (ACLs)', 'Block public access to buckets and objects granted through new public bucket or access point policies', 'Block public and cross-account access to buckets and objects through any public bucket or access point policies', and 'Block public access to buckets and objects through new access point policies'. All these checkboxes are also unchecked.

**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.**

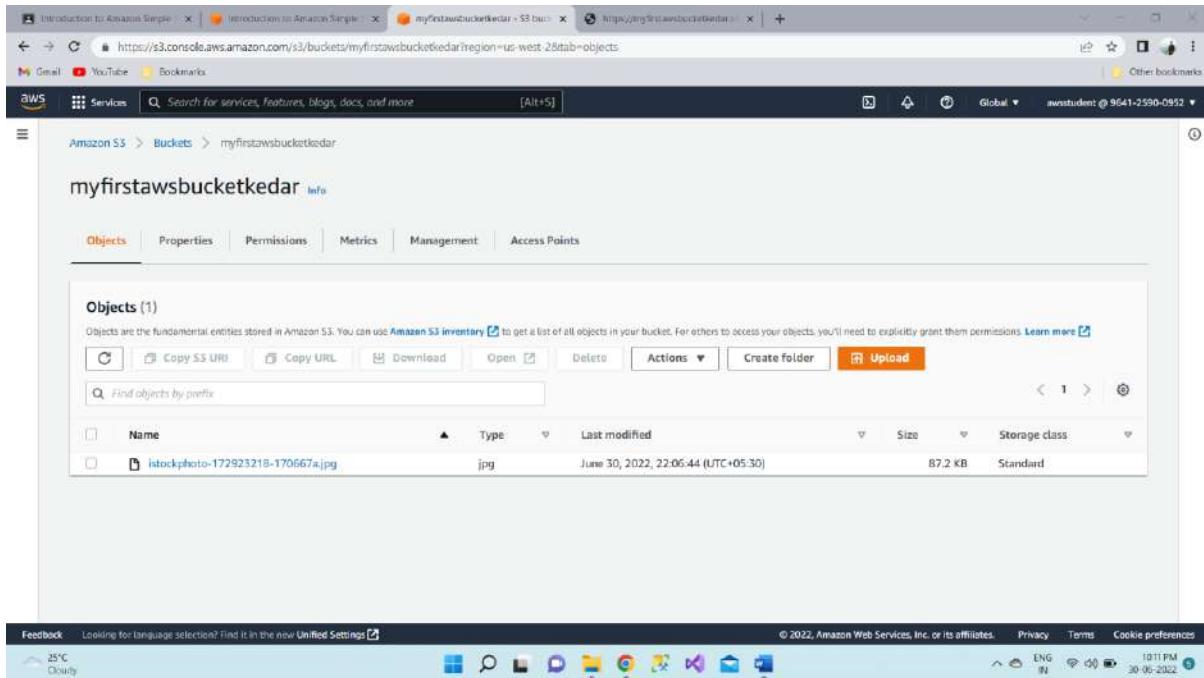


A Successfully edited bucket settings for Block Public Access message displays at the top of the window.

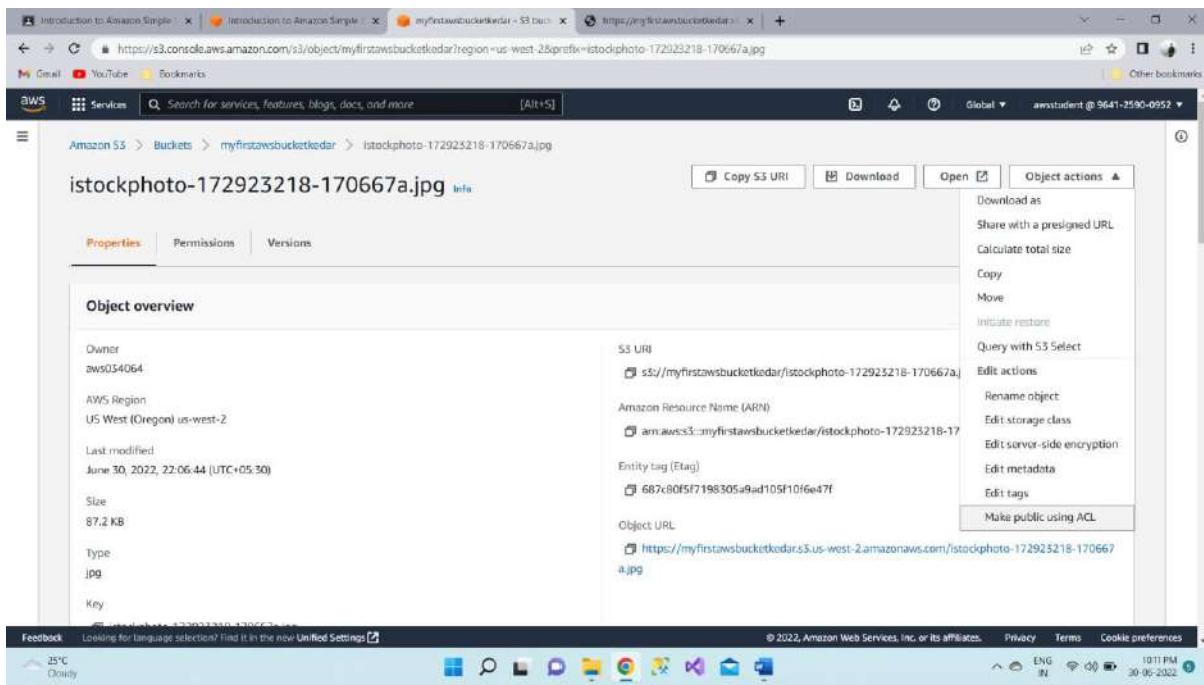


**Step 26 – Choose the Objects Tab.**

**Step 27 – Choose the File name.**

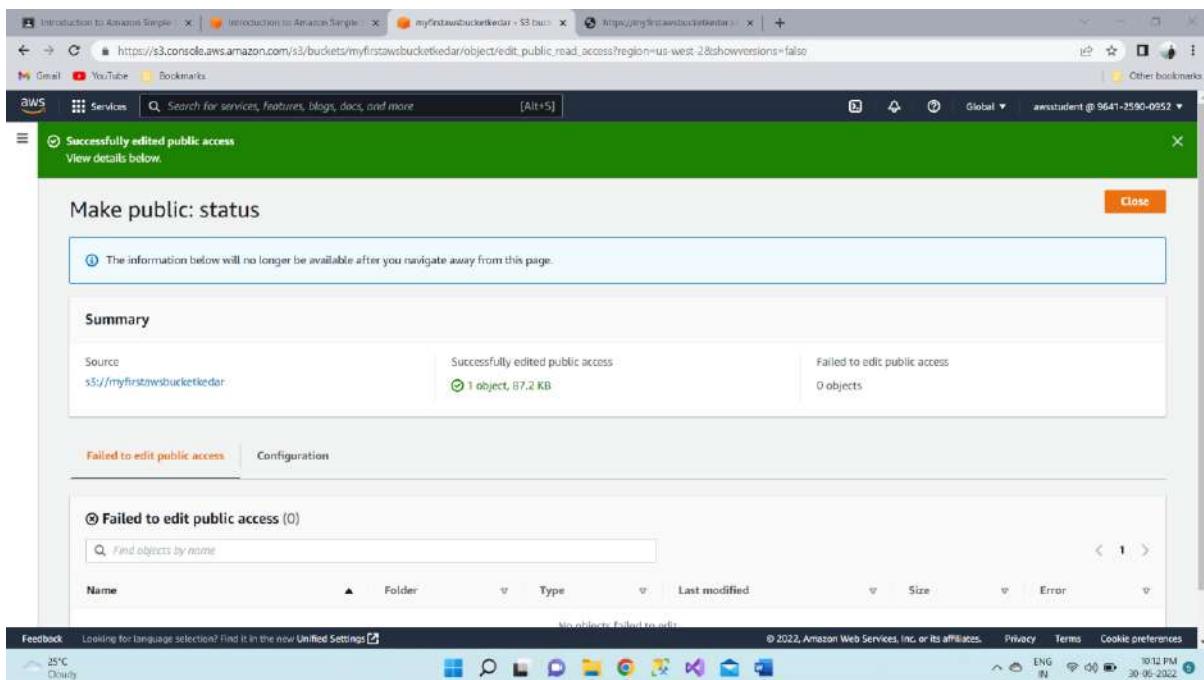


**Step 27** – On the new-report.png overview page, choose the Object actions button and select Make public via ACL.

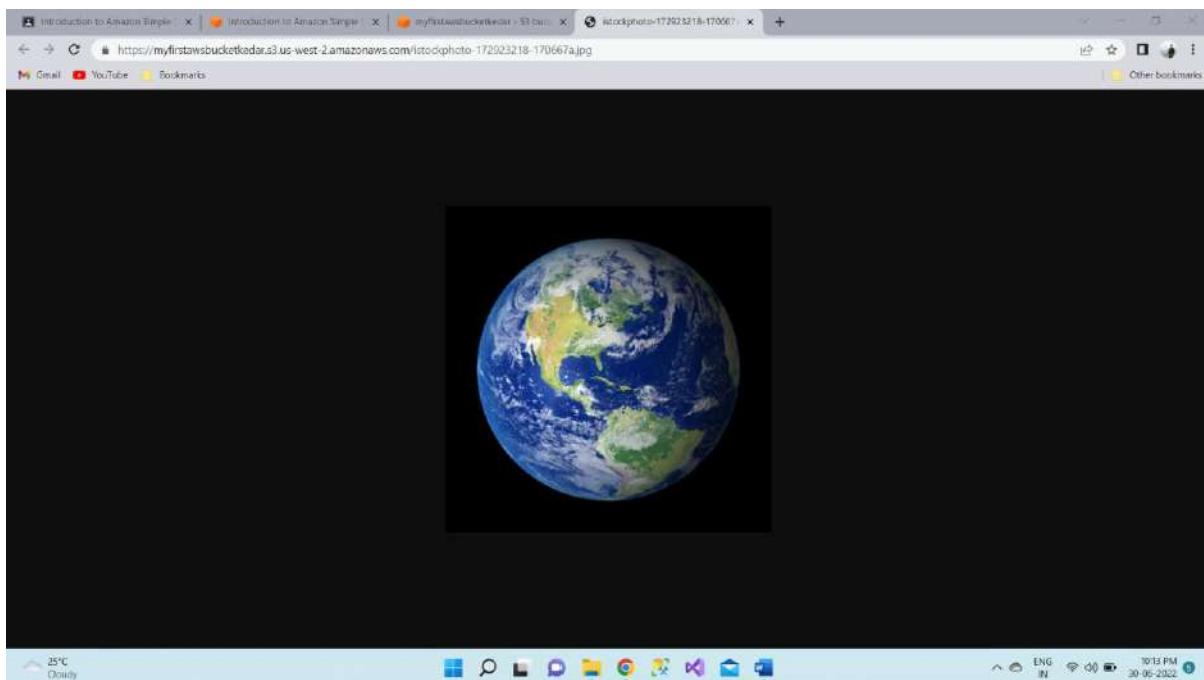


**Step 28** – Choose Make public and you should see the green banner Successfully edited public access at the top of the window.

**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.



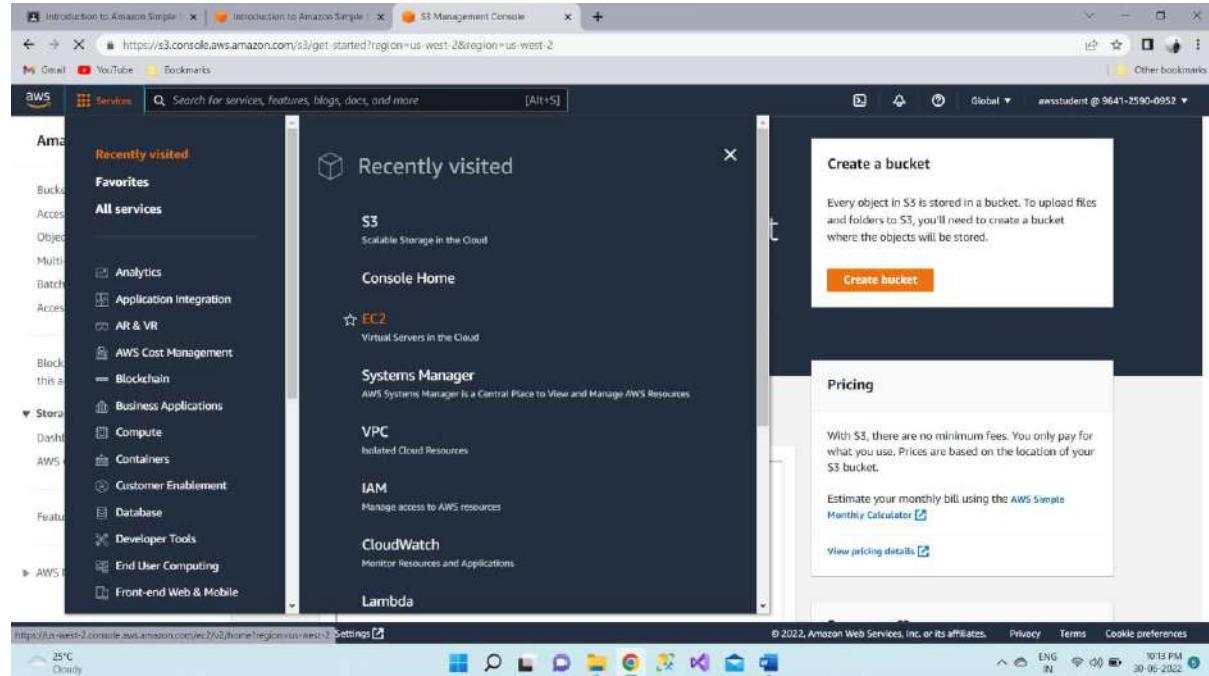
Close the web browser tab that displays your.png image and return to the tab with the Amazon S3 Management Console.

## Task 4: Test connectivity from the EC2 instance

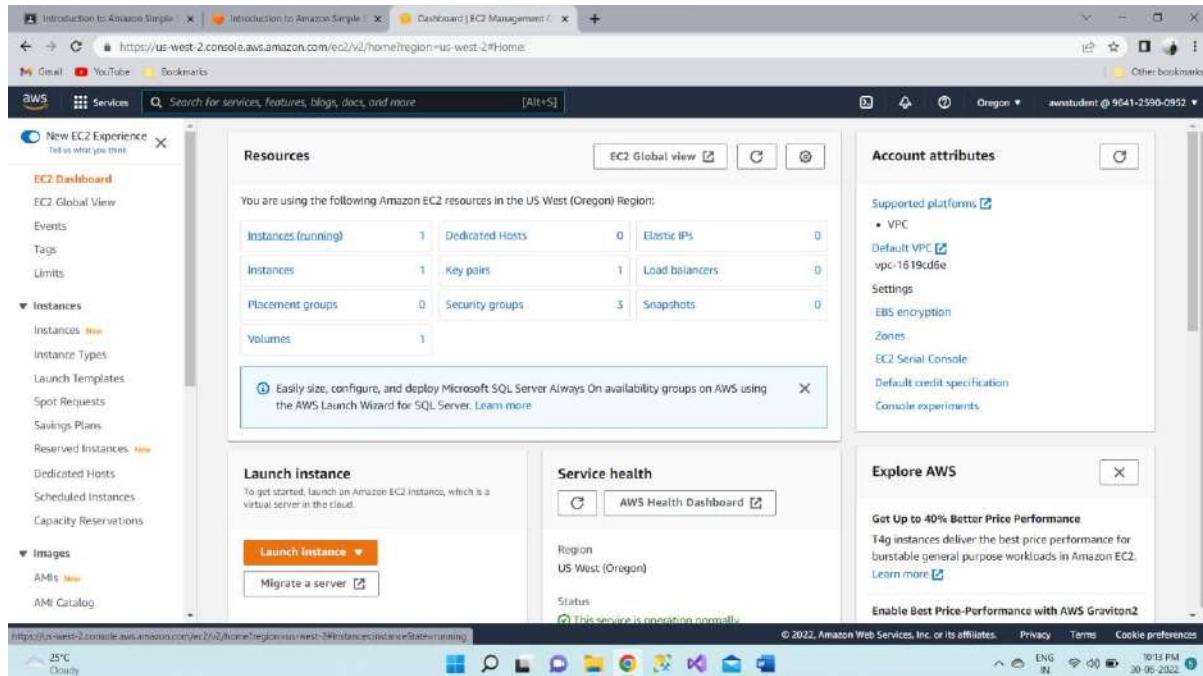
In this task, you connect to your Amazon Elastic Compute Cloud (Amazon EC2) instance to test connectivity and security to the S3 reportbucket.

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.

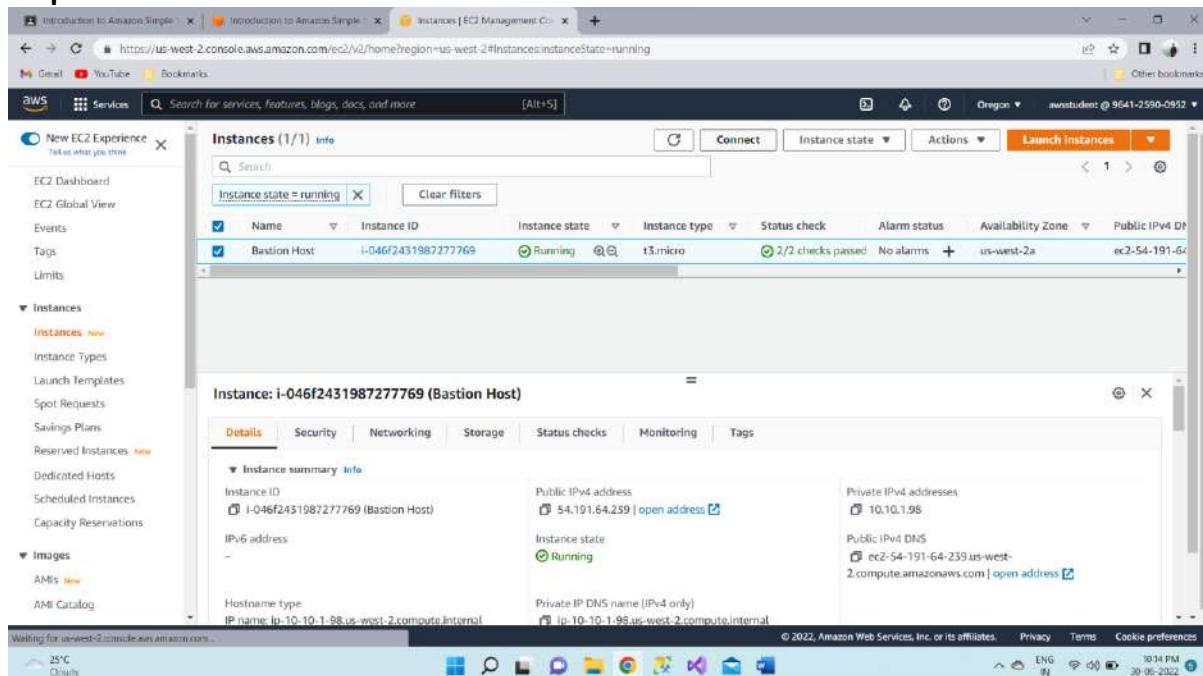
**Step 31** – On the service Menu choose EC2.



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

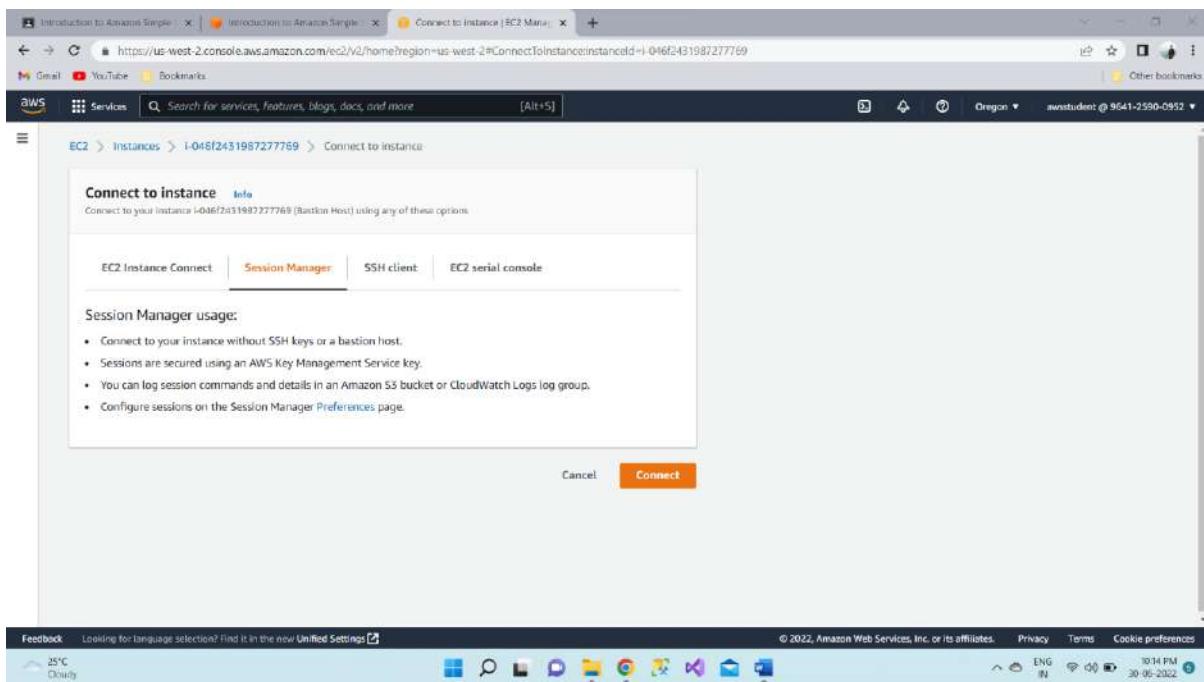


### Step 33 – Select Bastion Host and Select Connect.

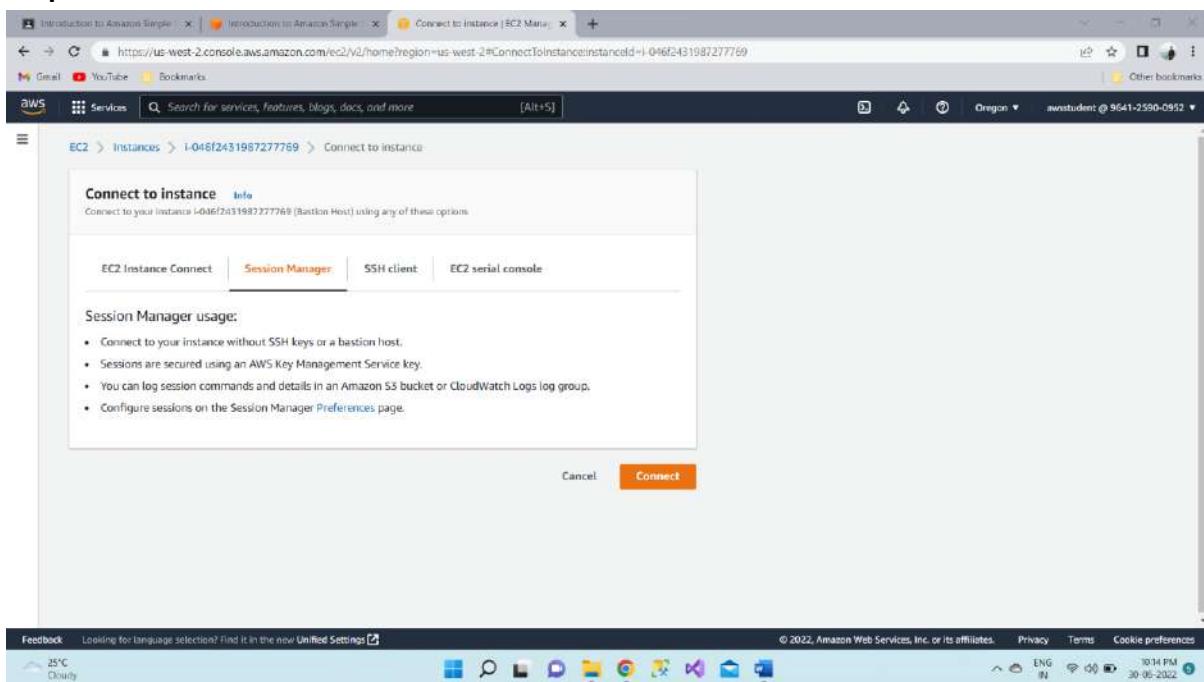


### Step 34 – In the Connect to instance window:

For Connection method, select Session Manager

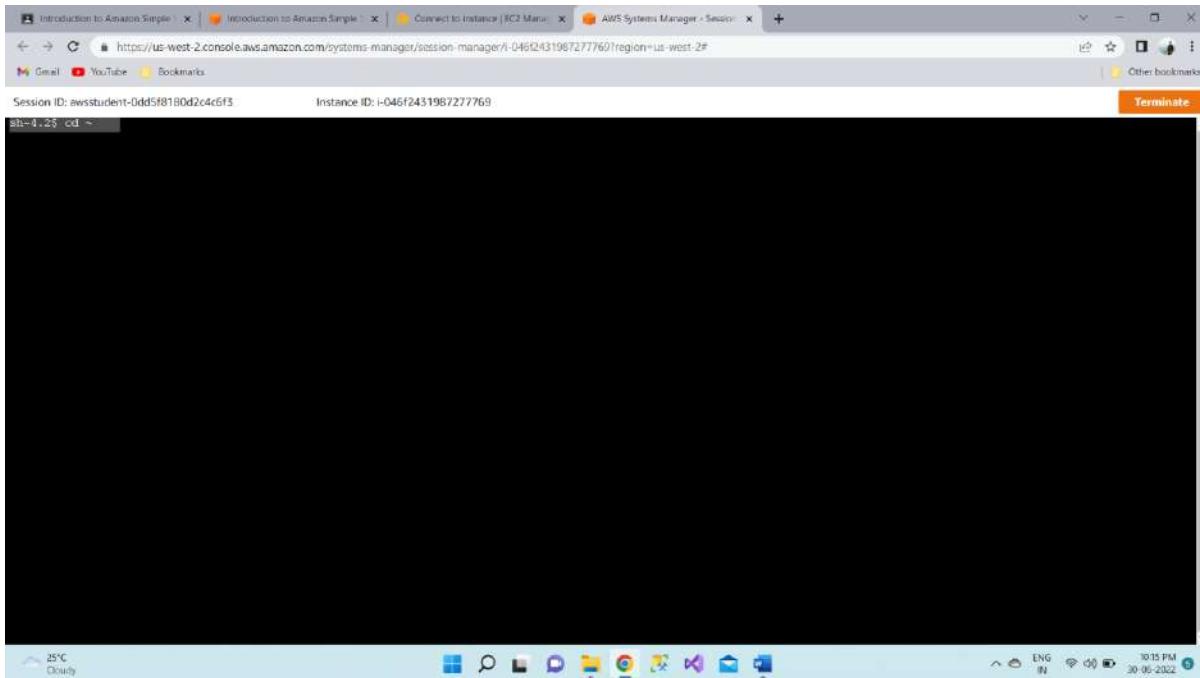


### Step 35 – Choose Connect.

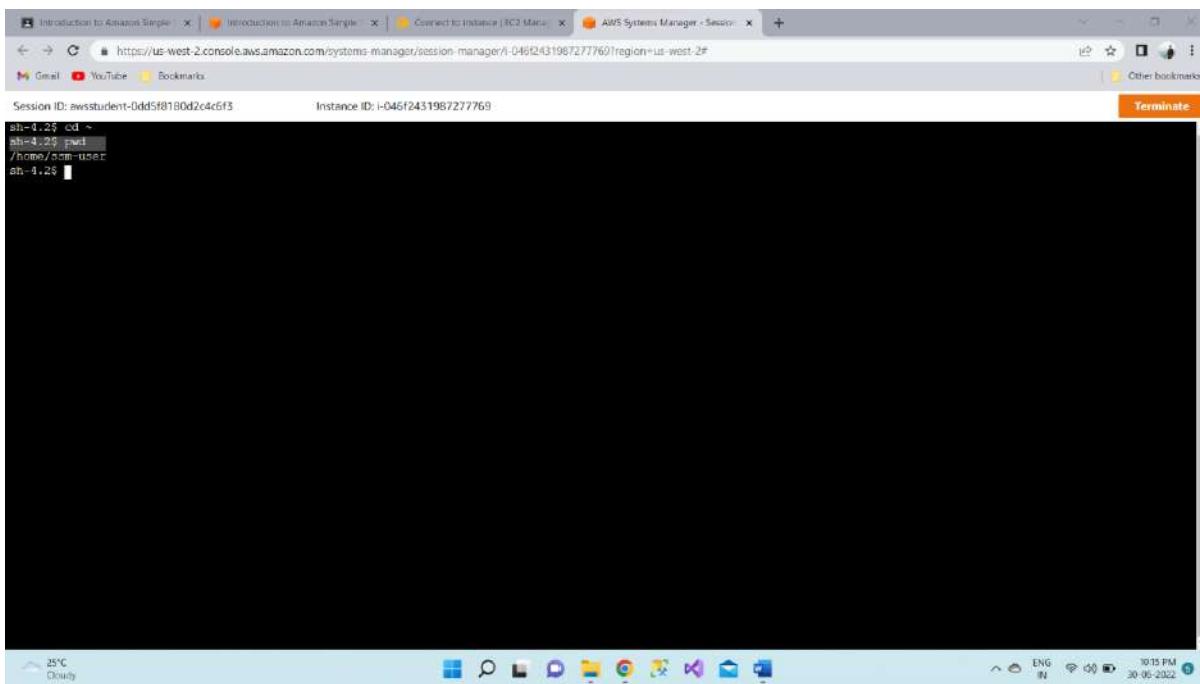


A new browser tab or window opens with a connection to the bastion host instance.

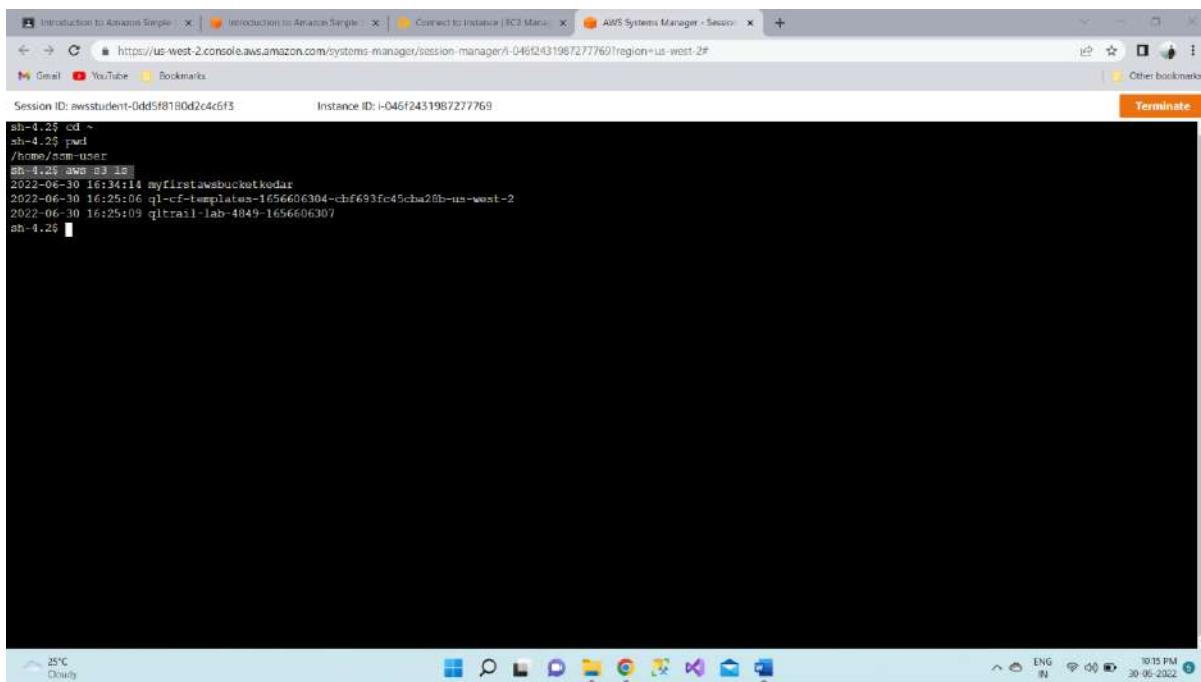
### Step 36 – In the bastion host session, enter the following command to change to home directory (/home/ssm-user/):



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



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



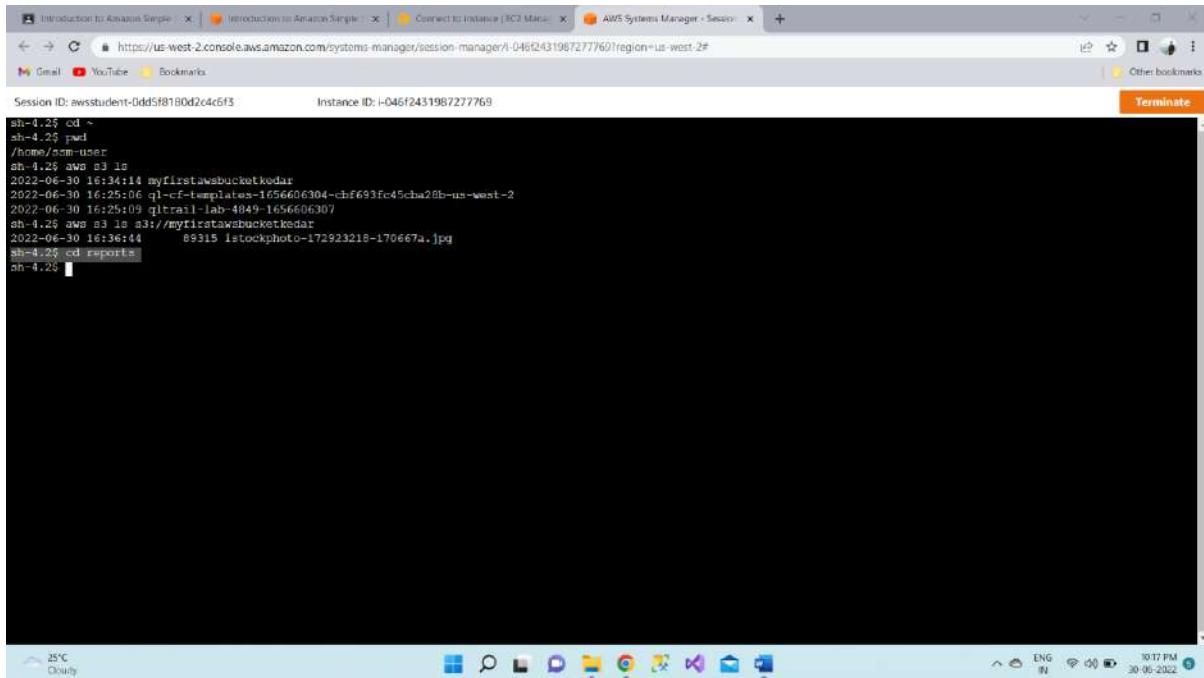
```
Session ID: awssstudent-0dd5f8180d2c4c6f3 Instance ID: i-046f2431987277769
sh-4.2$ cd ~
sh-4.2$ pwd
/home/awssstudent
sh-4.2$ aws s3 ls
2022-06-30 16:34:14 myFirstawsbucketkedar
2022-06-30 16:25:06 q1-cf-templates-1656606304-chf693fc45cba2fb-us-west-2
2022-06-30 16:25:09 qltrail-lab-4049-1656606307
sh-4.2$
```

You see the reportbucket 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.

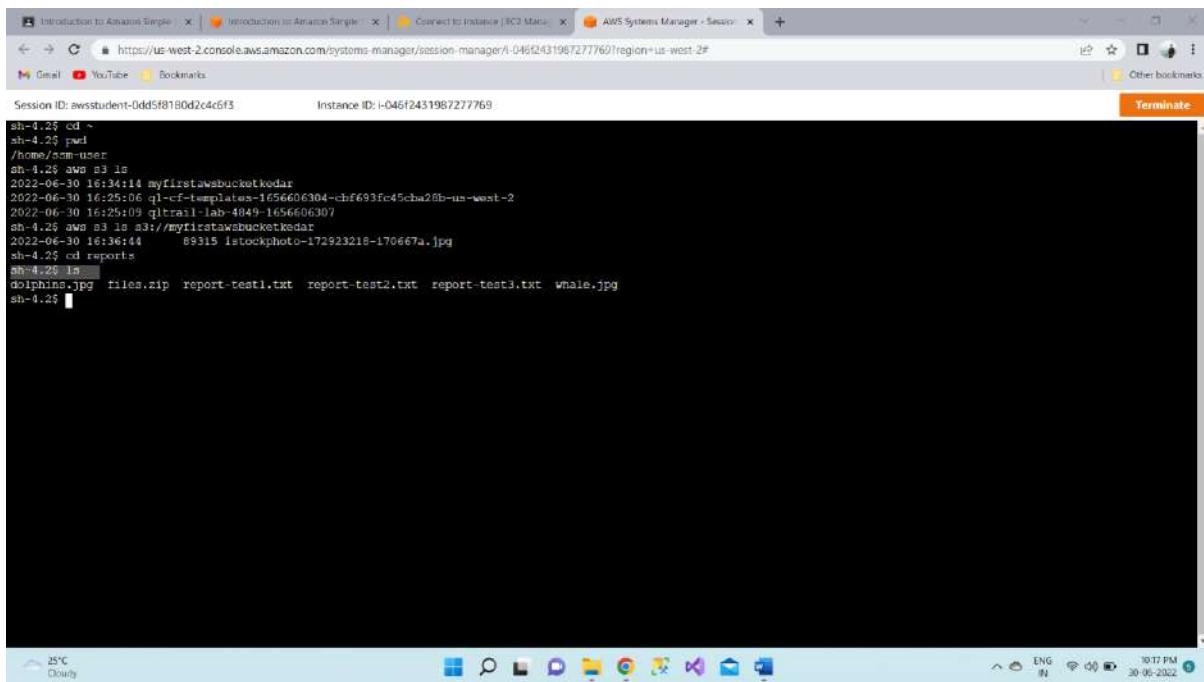
**Step 39** – Enter the following command to list all objects in your reportbucket. Remember to change the number at the end of the reportbucket name, to match the name of the bucket you created.

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



```
Session ID: awssstudent-Ddd5f8180d2c4c6f3 Instance ID: i-046f2431987277769
sh-4.2$ cd ~
sh-4.2$ pwd
/home/sum-user
sh-4.2$ aws s3 ls
2022-06-30 16:34:14 myfirstawsbucketkedar
2022-06-30 16:25:06 ql-cf-templates-1656606304-chf693fc45cha2bb-us-west-2
2022-06-30 16:25:09 qltrail-lab-4849-1656606307
sh-4.2$ aws s3 ls s3://myfirstawsbucketkedar
2022-06-30 16:36:44 89315 istockphoto-172923218-170667a.jpg
sh-4.2$ cd reports
sh-4.2$ ls
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt whale.jpg
sh-4.2$
```

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



```
Session ID: awssstudent-Ddd5f8180d2c4c6f3 Instance ID: i-046f2431987277769
sh-4.2$ cd ~
sh-4.2$ pwd
/home/sum-user
sh-4.2$ aws s3 ls
2022-06-30 16:34:14 myfirstawsbucketkedar
2022-06-30 16:25:06 ql-cf-templates-1656606304-chf693fc45cha2bb-us-west-2
2022-06-30 16:25:09 qltrail-lab-4849-1656606307
sh-4.2$ aws s3 ls s3://myfirstawsbucketkedar
2022-06-30 16:36:44 89315 istockphoto-172923218-170667a.jpg
sh-4.2$ cd reports
sh-4.2$ ls
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt whale.jpg
sh-4.2$
```

**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.

```

Session ID: awssstudent-0dd5f8180d2c4c6f3           Instance ID: i-046f2431987277769
Session ID: awssstudent-0dd5f8180d2c4c6f3           Instance ID: i-046f2431987277769
aws-4.2$ cd ~
aws-4.2$ pwd
/home/sam-user
aws-4.2$ aws s3 ls
2022-06-30 16:34:14 myfirstawsbucketkedar
2022-06-30 16:25:06 s3://myfirstawsbucketkedar
aws-4.2$ aws s3 ls s3://myfirstawsbucketkedar
2022-06-30 16:36:44      69315 istockphoto-172923218-170667a.jpg
aws-4.2$ cd reports
aws-4.2$ ls
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt whale.jpg
aws-4.2$ aws s3 cp report-test1.txt s3://myfirstawsbucketkedar
upload failed: ./report-test1.txt to s3://myfirstawsbucketkedar/report-test1.txt An error occurred (AccessDenied) when calling the PutObject operation: Access Denied
aws-4.2$ 

```

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.

```

Session ID: awssstudent-0dd5f8180d2c4c6f3           Instance ID: i-046f2431987277769
Session ID: awssstudent-0dd5f8180d2c4c6f3           Instance ID: i-046f2431987277769
aws-4.2$ cd ~
aws-4.2$ pwd
/home/sam-user
aws-4.2$ aws s3 ls
2022-06-30 16:34:14 myfirstawsbucketkedar
2022-06-30 16:25:06 s3://myfirstawsbucketkedar
aws-4.2$ aws s3 ls s3://myfirstawsbucketkedar
2022-06-30 16:36:44      69315 istockphoto-172923218-170667a.jpg
aws-4.2$ cd reports
aws-4.2$ ls
dolphins.jpg files.zip report-test1.txt report-test2.txt report-test3.txt whale.jpg
aws-4.2$ aws s3 cp report-test1.txt s3://myfirstawsbucketkedar
upload failed: ./report-test1.txt to s3://myfirstawsbucketkedar/report-test1.txt An error occurred (AccessDenied) when calling the PutObject operation: Access Denied
aws-4.2$ 

```

## Practical 4: Introduction to AWS Key management Service

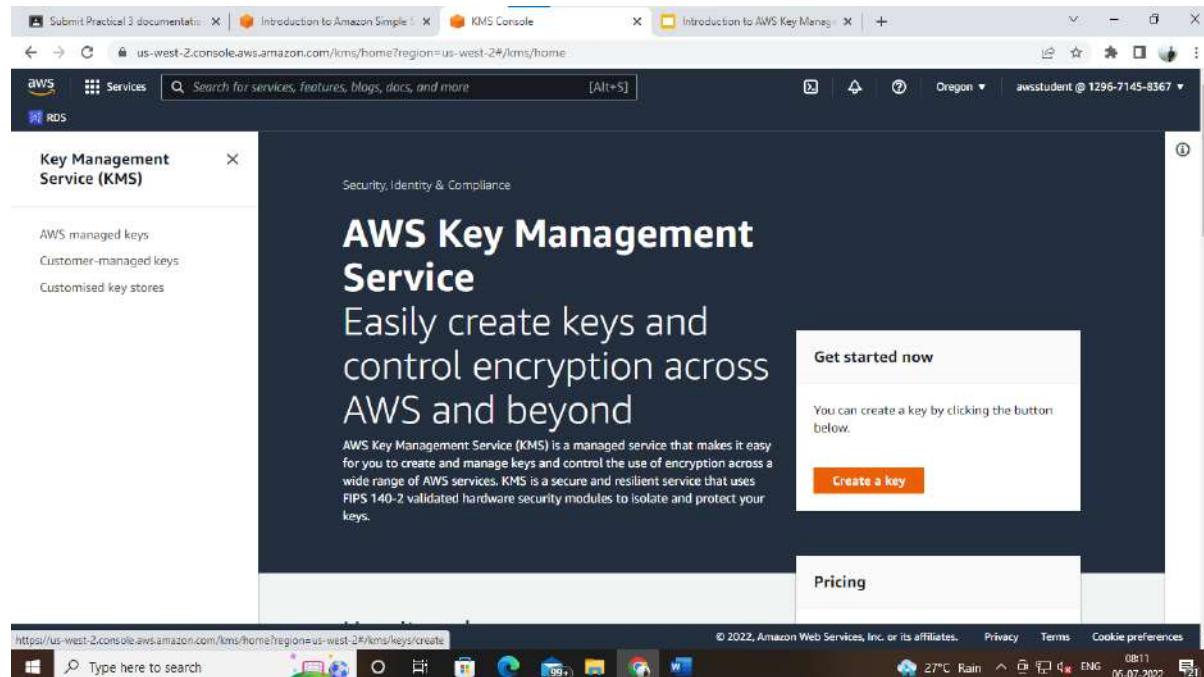
- A. Create KMS master key**
- B. Configure CloudTrail to store Logs in an S3 Bucket**
- C. Upload an Image to S3 bucket and encrypt it**
- D. Access the encrypted image**
- E. Monitor KMS activity Using CloudTrail Logs**
- F. Manage encryption keys**

## Task 1: Create Your KMS Master Key

### Step 1 – Start Lab and click on Open Console

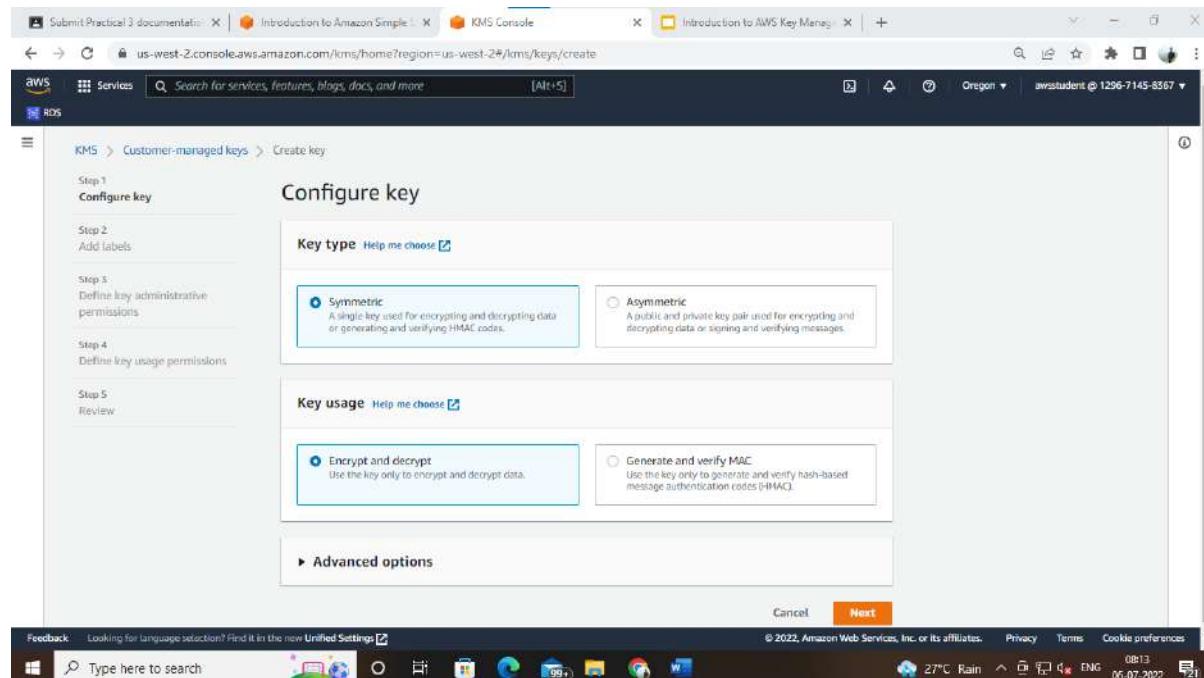
### Step 2 – Start Lab and click on Open Console

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



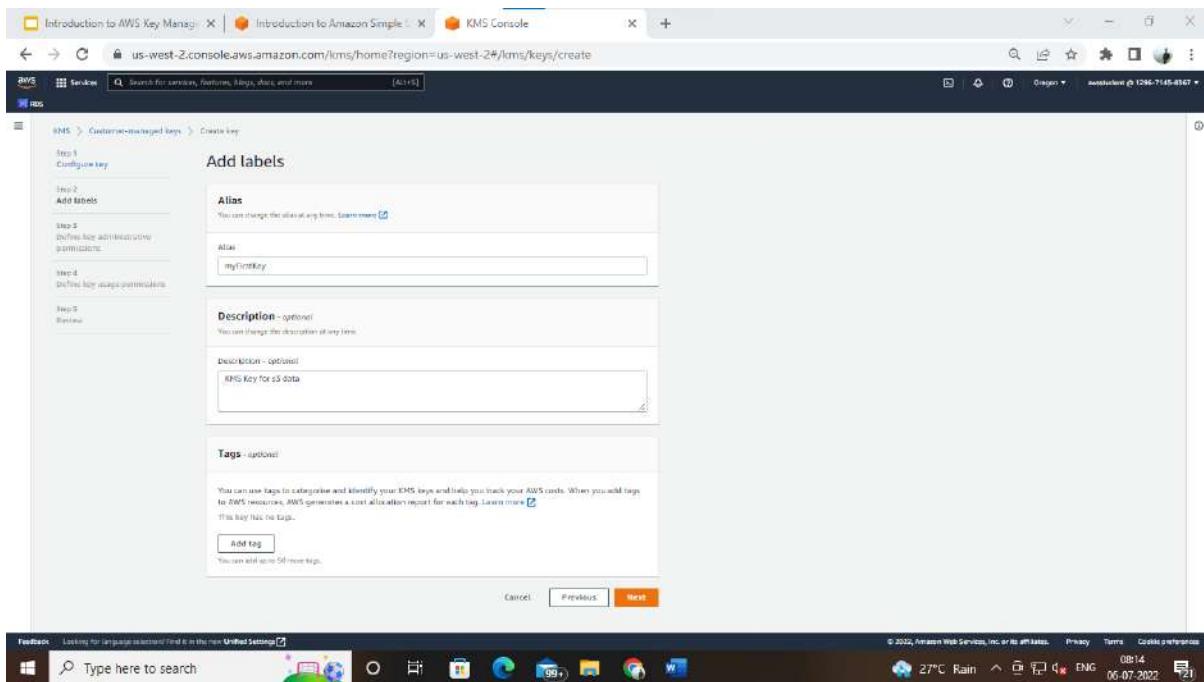
**Step 4 – Click Create a key the configure:**

- On the Configure Key page Select Symmetric
- Click Next



**Step 5 – On the Add Labels page configure:**

- **Alias:** myFirstKey
- **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.**

The screenshot shows the AWS KMS 'Create Key' wizard at Step 3: Define key administrative permissions. The left sidebar lists steps: Step 1: Configure key, Step 2: Add labels, Step 3: Define key administrative permissions (which is active), Step 4: Define key usage permissions, and Step 5: Review. The main area is titled 'Define key administrative permissions' and contains a table titled 'Key administrators'. The table lists IAM entities with their names, paths, and types. The entity 'awsstudent' is selected and highlighted with a blue border. Other listed entities include root-qwkl, AWSBatchServiceRole, AWSServiceRoleForAmazonElasticSearchService, AWSServiceRoleForAPIGateway, AWSServiceRoleForAutoScaling, AWSServiceRoleForAWSCloud9, AWSServiceRoleForAWSLicenseManagerMasterAccountRole, AWSServiceRoleForAWSLicenseManagerRole, and AWSServiceRoleForDAX. Below the table is a 'Key deletion' section with a checkbox labeled 'Allow key administrators to delete this key.' At the bottom are 'Cancel', 'Previous', and 'Next' buttons.

**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.

The screenshot shows the 'Define key usage permissions' step of the AWS KMS 'Create Key' wizard. The left sidebar lists steps 1 through 5: Configure key, Add labels, Define key administrative permissions, Define key usage permissions (which is currently selected), and Review. The main area is titled 'Define key usage permissions' and contains two sections: 'This account' and 'Other AWS accounts'. In the 'This account' section, a table lists IAM entities with checkboxes for selection. The 'awsstudent' user is checked. Other listed entities include root-qwkl1, AWSBatchServiceRole, AWSServiceRoleForAmazonElasticSearchService, AWSServiceRoleForAPIGateway, AWSServiceRoleForAutoScaling, AWSServiceRoleForAWSCloud9, AWSServiceRoleForAWSLicenseManagerMasterAccountRole, AWSServiceRoleForAWSLicenseManagerRole, and AWSServiceRoleForDAX. Below the table is a note about selecting IAM users and roles that can use the KMS key in cryptographic operations. At the bottom of the page are 'Cancel', 'Previous', and 'Next' buttons.



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

- Review the key policy
- Click Finish.

**Key configuration**

- Key type: Symmetric
- Key spec: SYMMETRIC\_DEFAULT
- Key usage: Encrypt and decrypt
- Origin: AWS KMS
- Regionality: Single-region key

**Alias and description**

- Alias: myFirstKey
- Description: KMS Key for s3 data

**Tags**

Key	Value
No data No tags to display	

**Key policy**

```

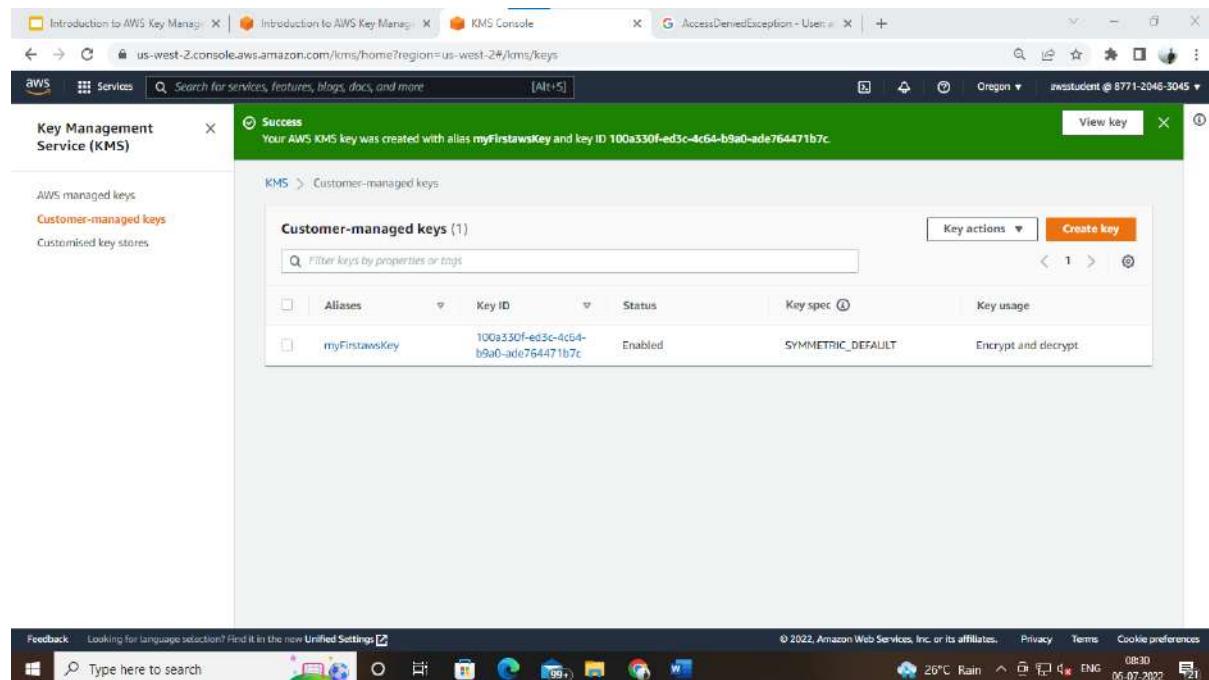
1: {
2:   "Id": "key-consolepolicy-3",
3:   "Version": "2012-10-17",
4:   "Statement": [
5:     {
6:       "Sid": "Enable IAM User Permissions",
7:       "Effect": "Allow",
8:       "Principal": {
9:         "AWS": "arn:aws:iam::129671498367:root"
10:      },
11:      "Action": "kms:*",
12:      "Resource": "*"
13:    },
14:    {
15:      "Sid": "Allow access for Key Administrators",
16:      ...
17:    }
18:  ]
19: }

```

Cancel Previous Finish

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

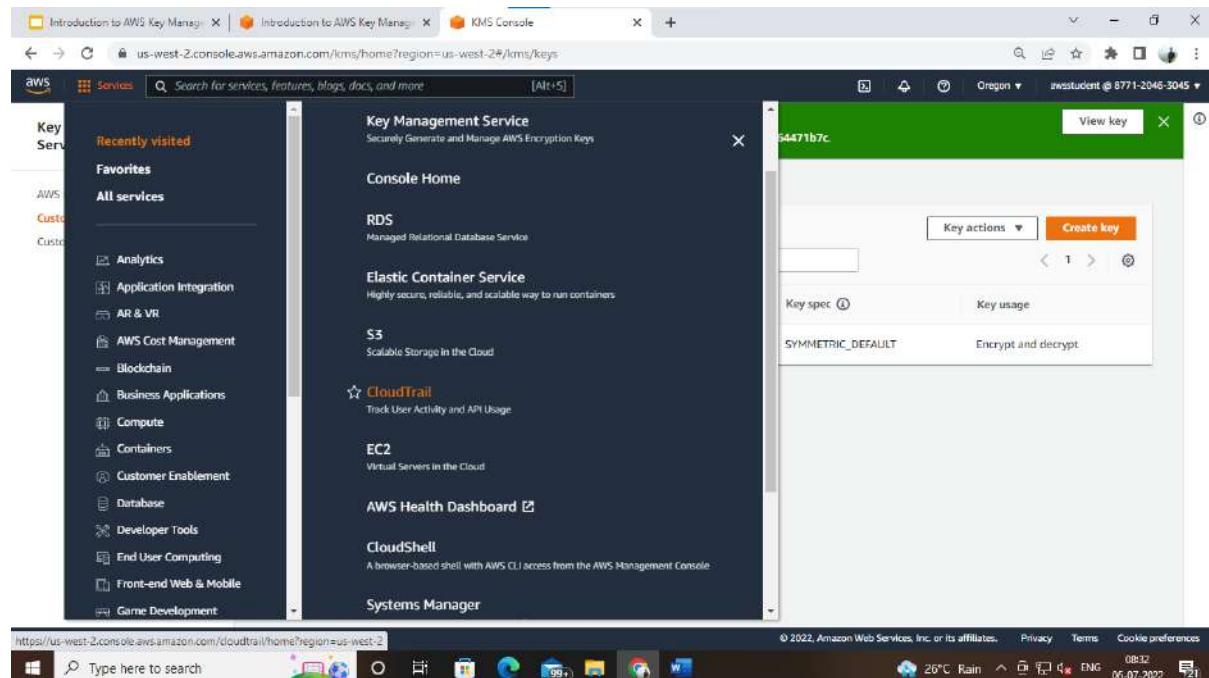
You will use this key id later when looking at the Log activities for this KMS key.



## 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.

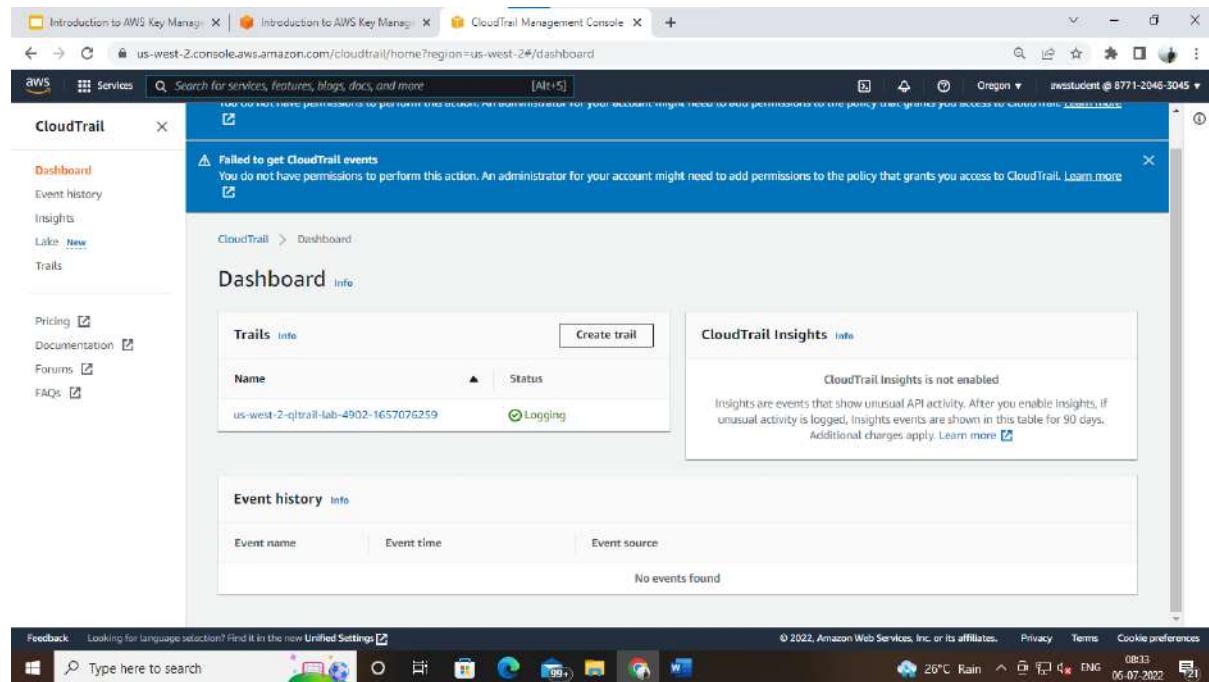
**Step 15** – If you see You do not have permission to perform this action. An administrator for your account might need to add permission to the policy that grants you access to Cloud Trail, you can ignore this warning.

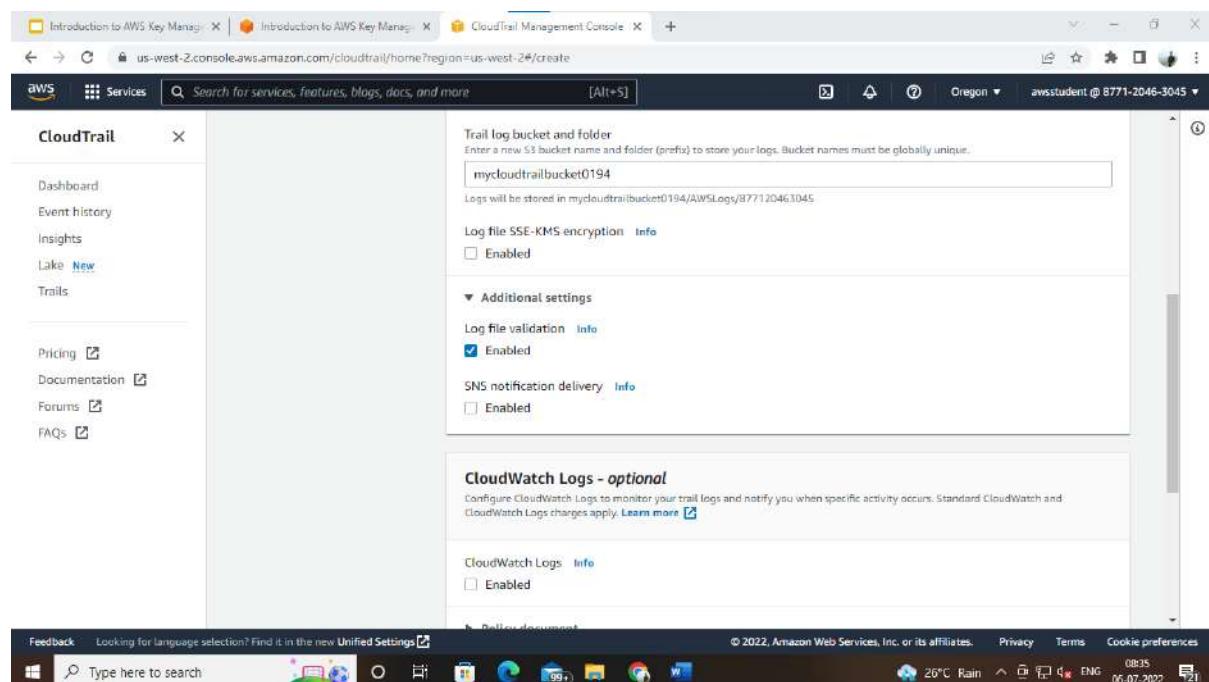
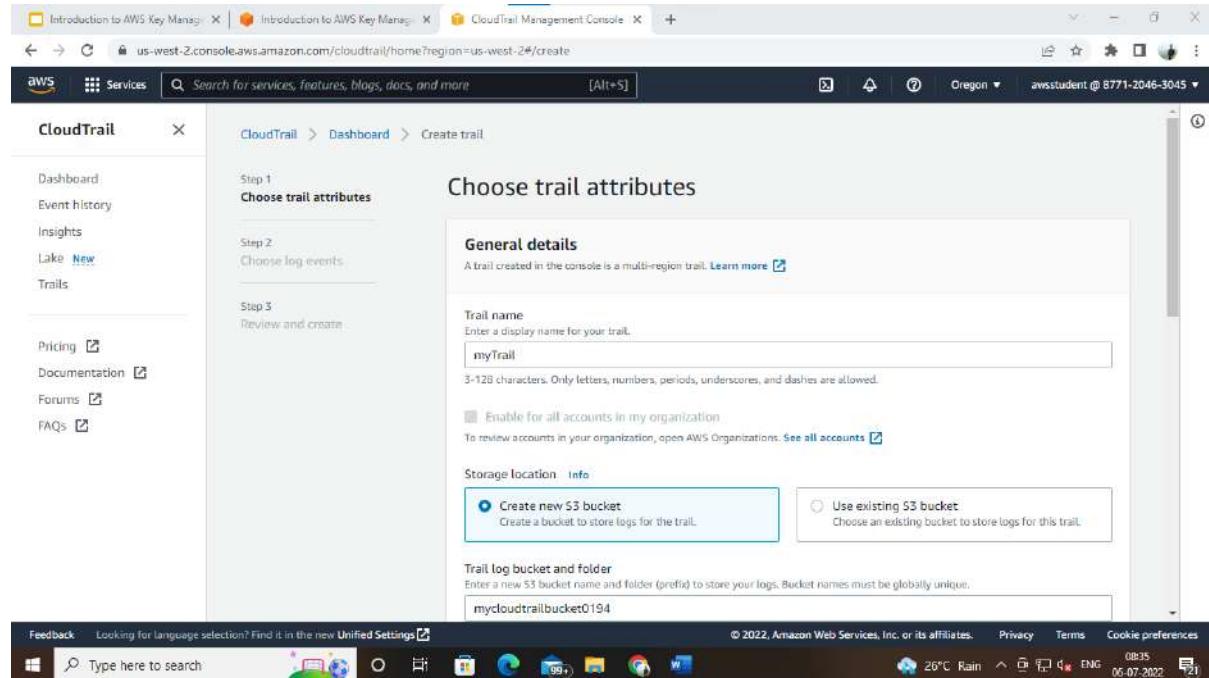
**Step 16** – In the navigation pane on the left, click Trails.

**Step 17** – Click Create trail then configure:

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

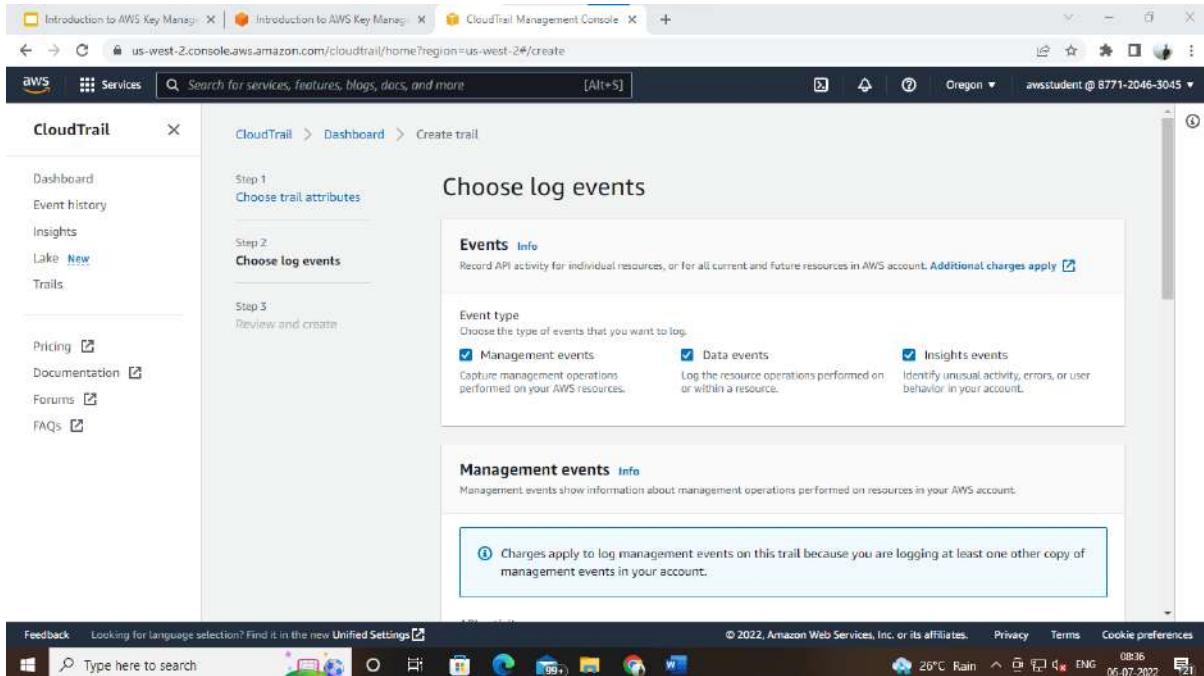
**Step 18** – Click Next.



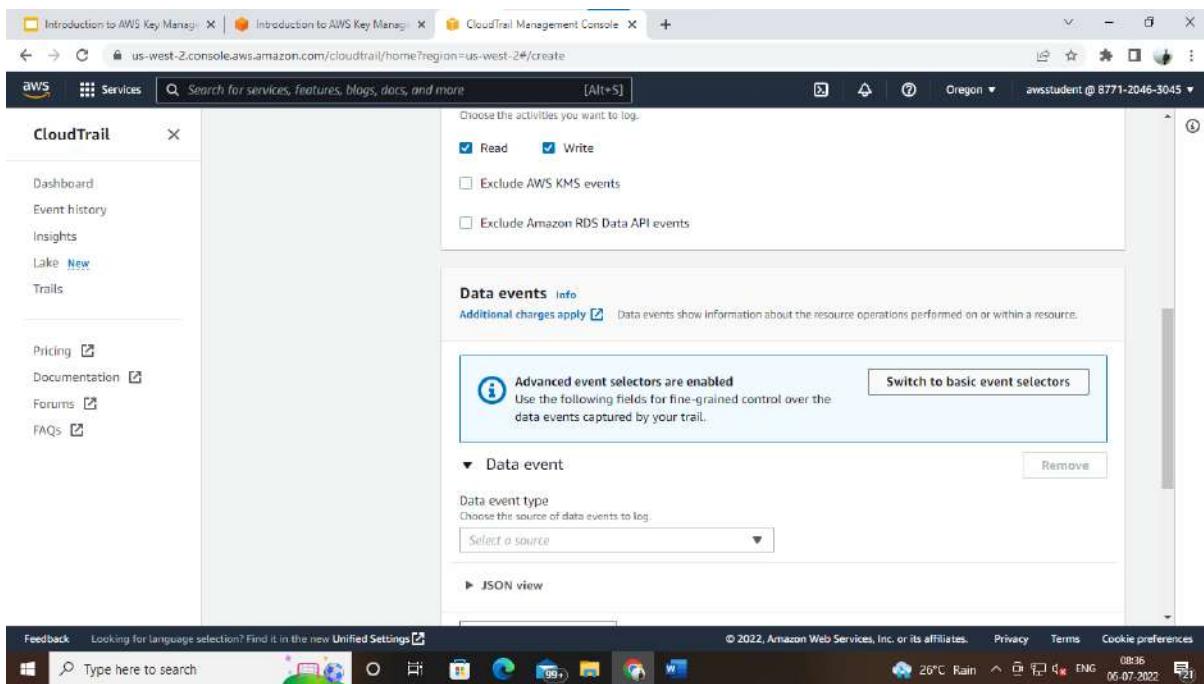


### Step 19 – On the Choose Log events page, configure:

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

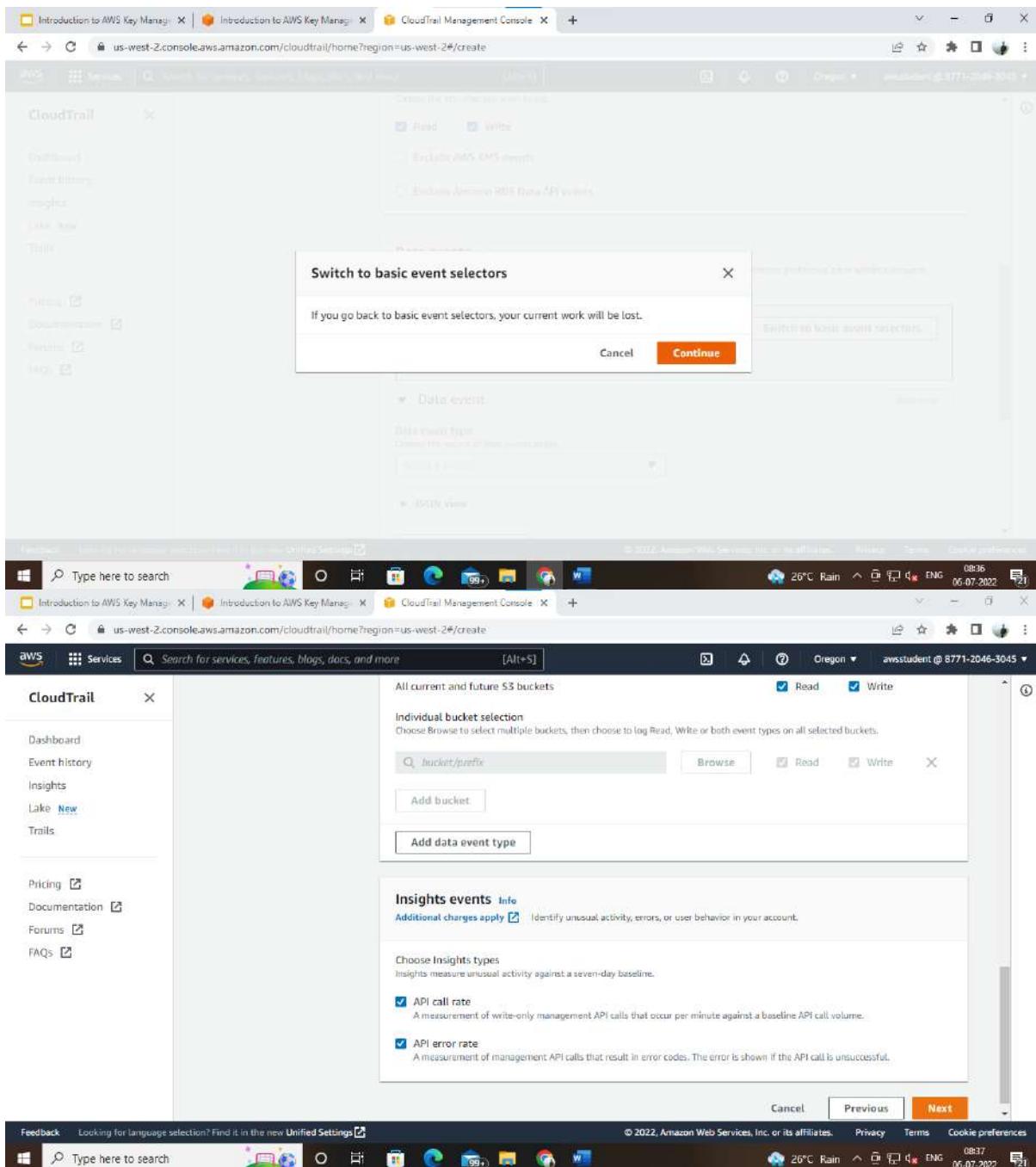


## Step 20 – In the Data events, Select Switch to basic event selector.



## Step 21 – In the Insight event, Select

- ✓ API call rate
- ✓ API error rate



**Step 22 – Click Next.**

**Step 23 – Click Create trail.**

**Review and create**

**Step 1: Choose trail attributes**

General details			
Trail name	myTrail	Trail log location	mycloudtrailbucket0194/AWS Logs/877120463045
Multi-region trail	Yes	Log file SSE-KMS encryption	Not enabled
Apply trail to my organization	Not enabled	Log file validation	Enabled
SNS notification delivery	Disabled	CloudWatch Logs	
No CloudWatch Logs log groups			

**Step 2: Choose log events**

**Step 3: Review and create**

**Create trail**

**Feedback** Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

26°C Rain 08:37 06-07-2022

**Data events : S3 (1)**

Bucket name	Prefix	Read	Write
All current and future S3 buckets		Enabled	Enabled

**Insights events**

API call rate	API error rate
Enabled	Enabled

**Create trail**

**Feedback** Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

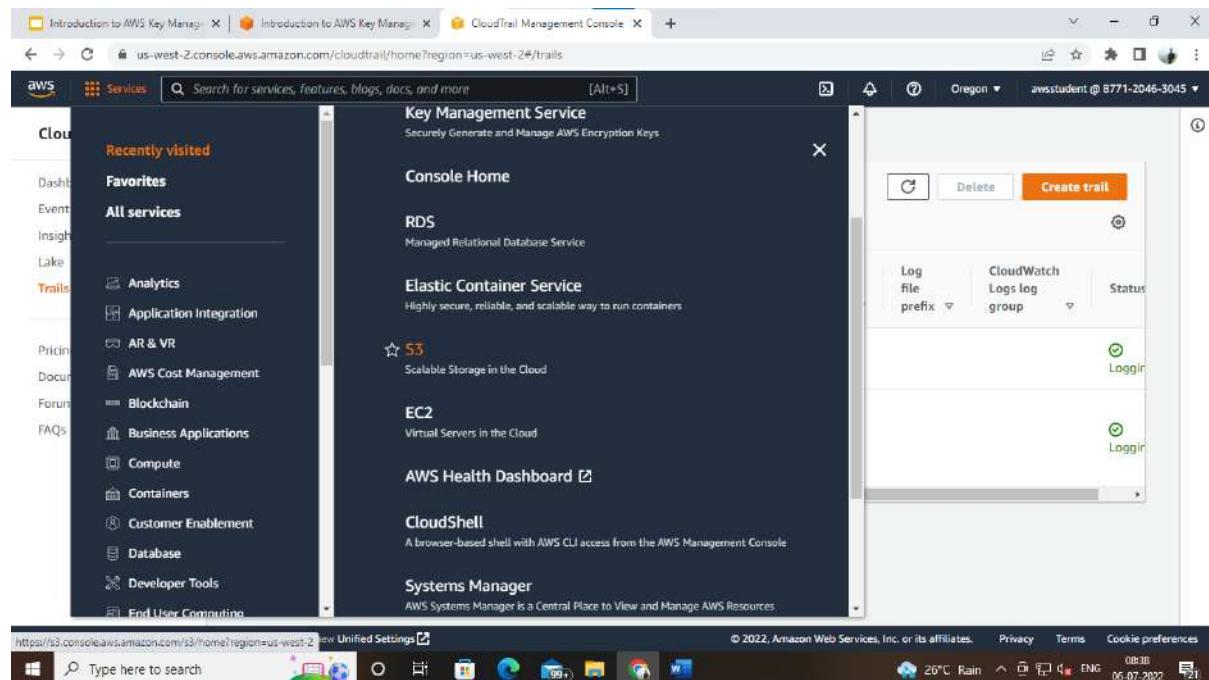
26°C Rain 08:37 06-07-2022

Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
myTrail	US West (Oregon)	Yes	Enabled	No	mycloudtrailbucket0194			
us-west-2-qtrail-lab-4902-1657076259	US West (Oregon)	No	Disabled	No	qtrail-lab-4902-1657076259			

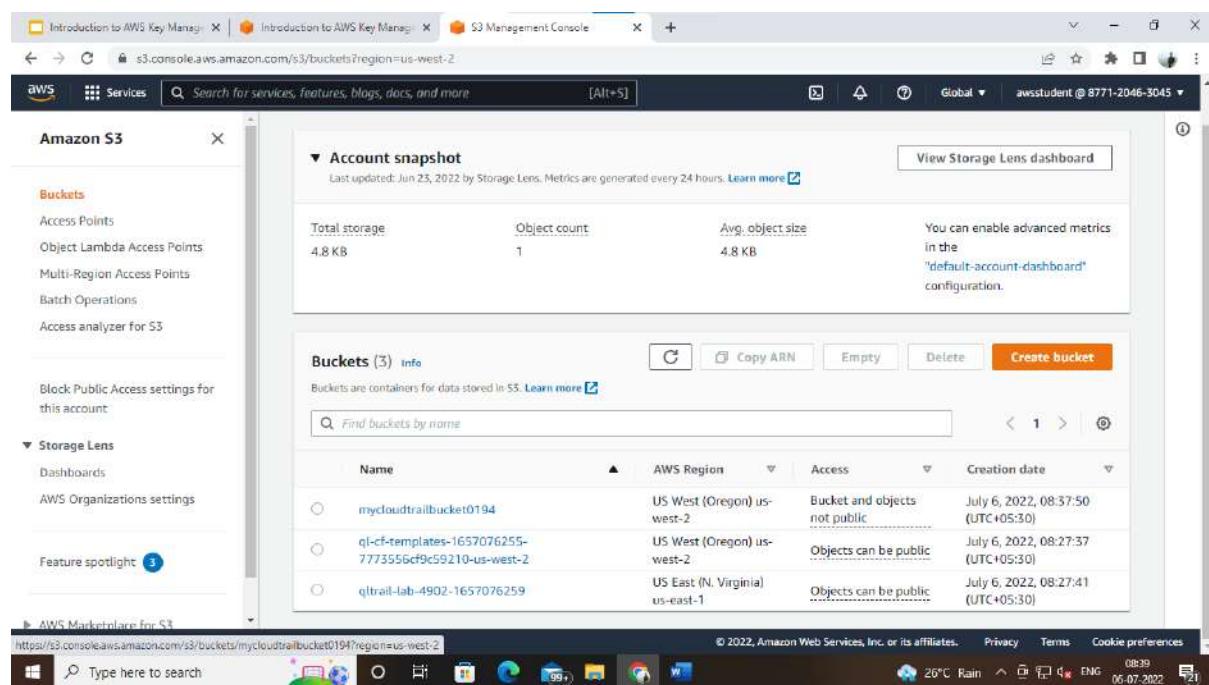
### Task 3: Upload an image to your S3 bucket and Encrypt It

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

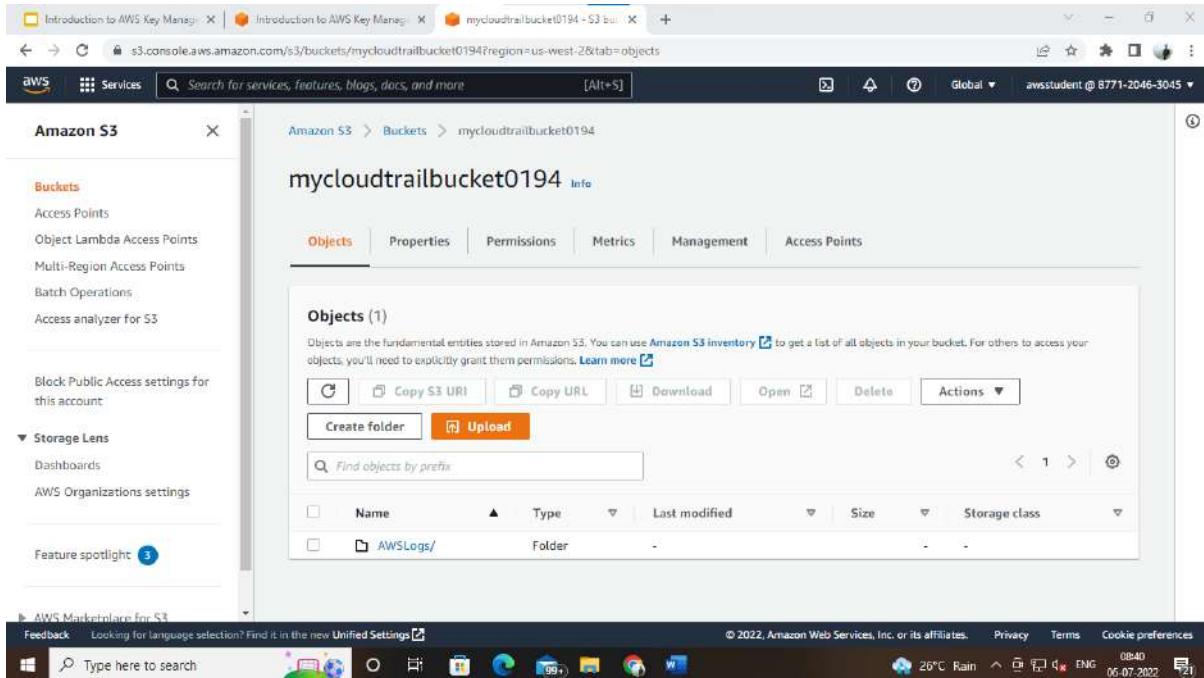
**Step 24** – On the Service Menu, click S3.



### Step 25 – Click mycloudtrailbucket\*.

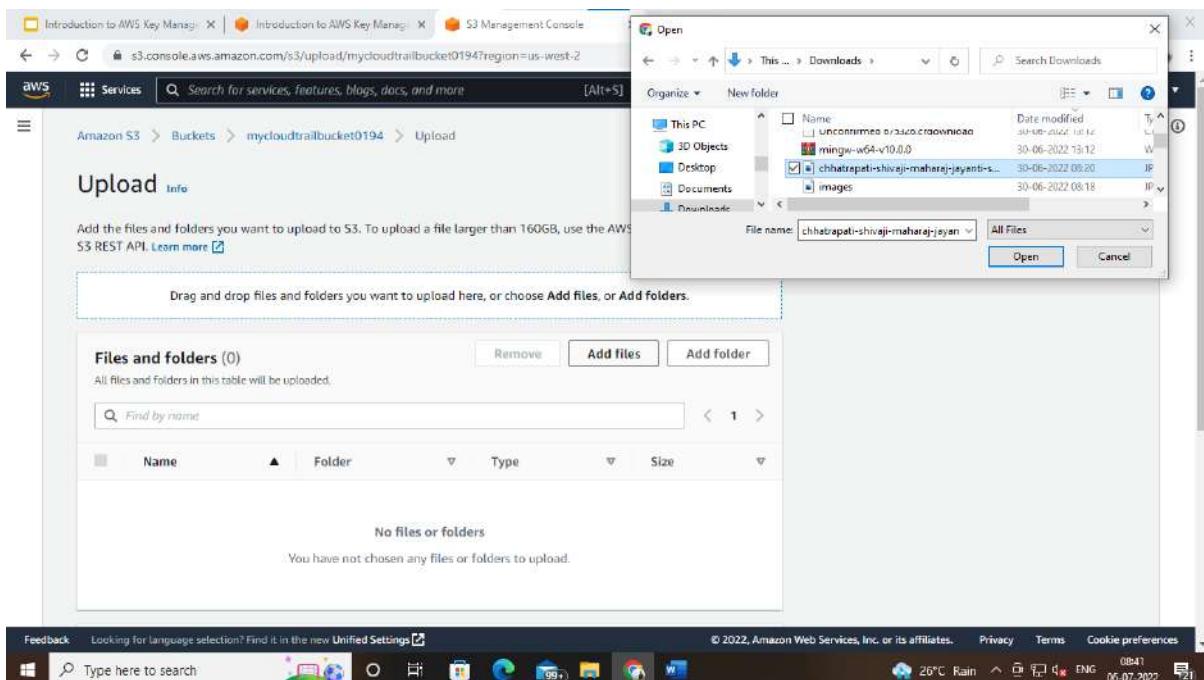


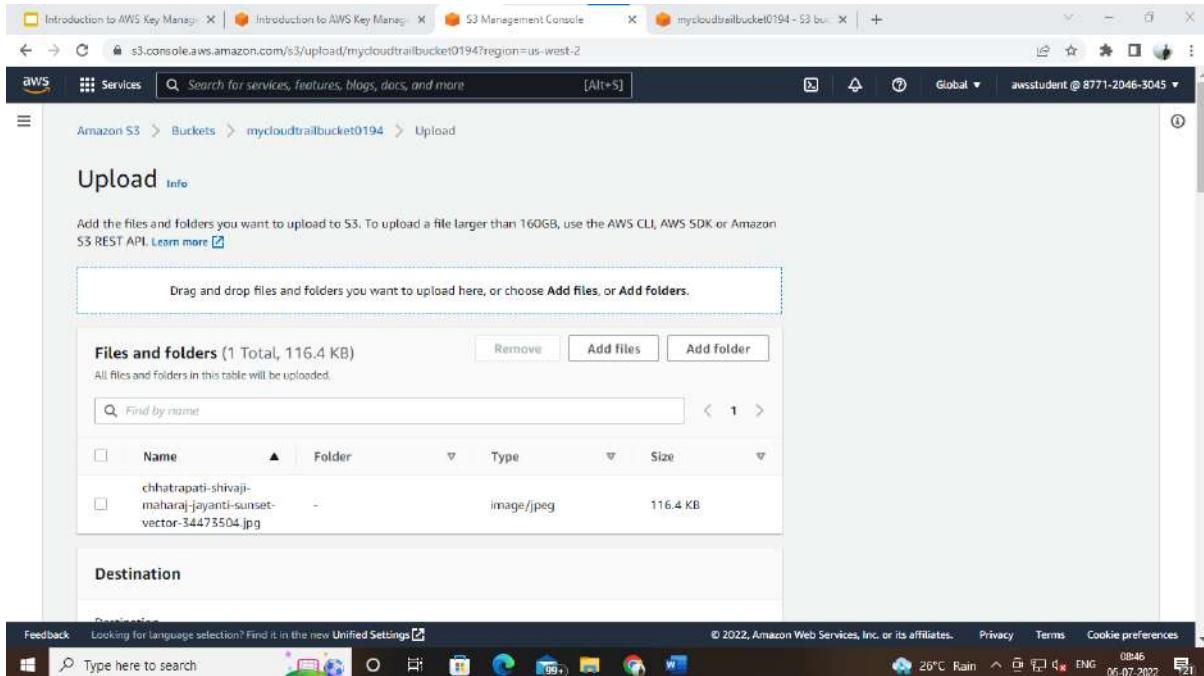
### Step 26 – From the objects tab, click Upload.



**Step 27** – Click Add files.

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



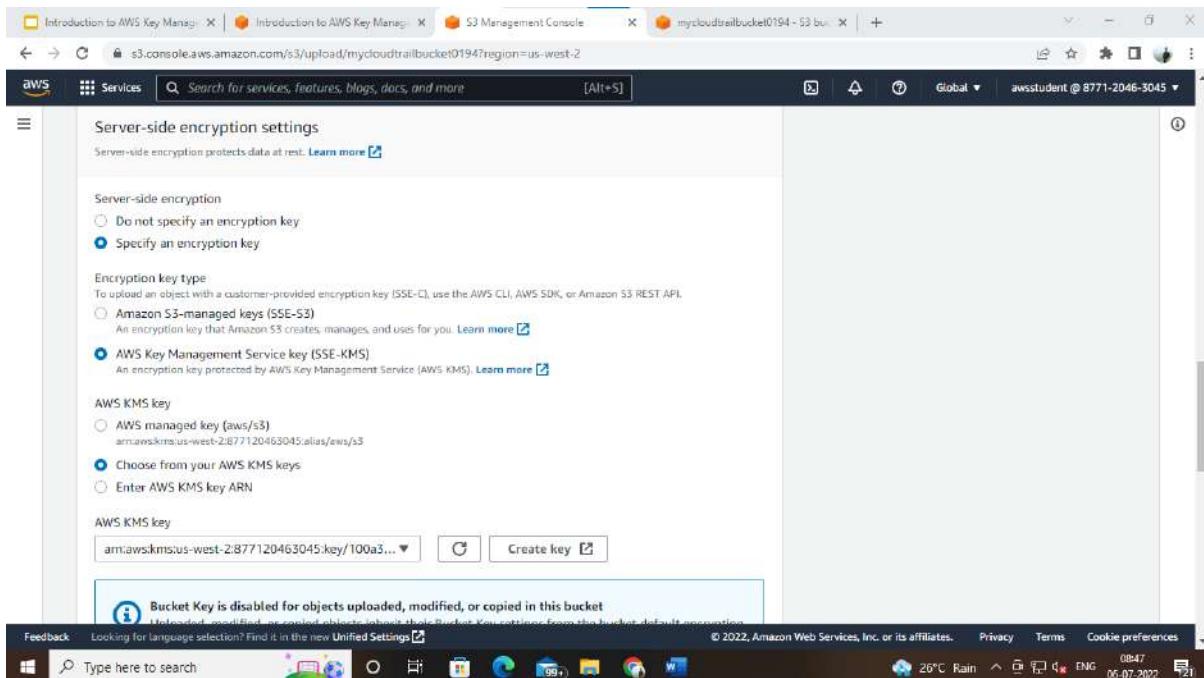


**Step 29** – At the bottom of the screen expand > **Properties**.

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

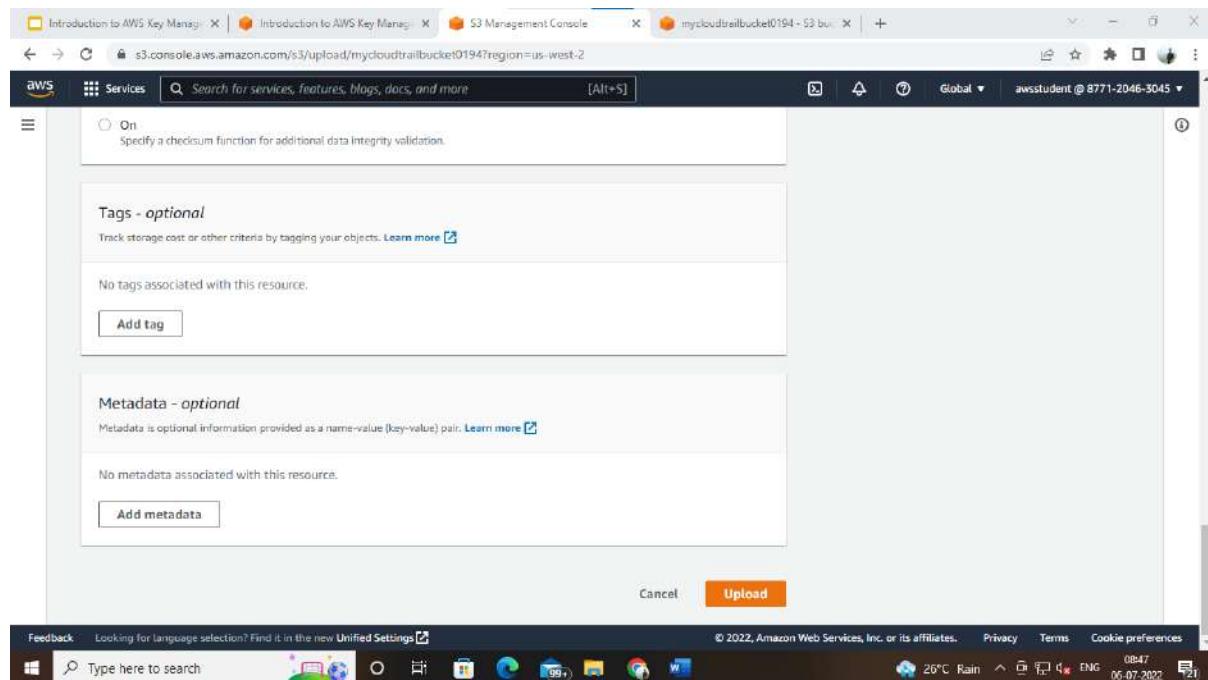
**Step 31** – For **Encryption Key Type**, Select **AWS Management Service Key (SSE- KMS)**.

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

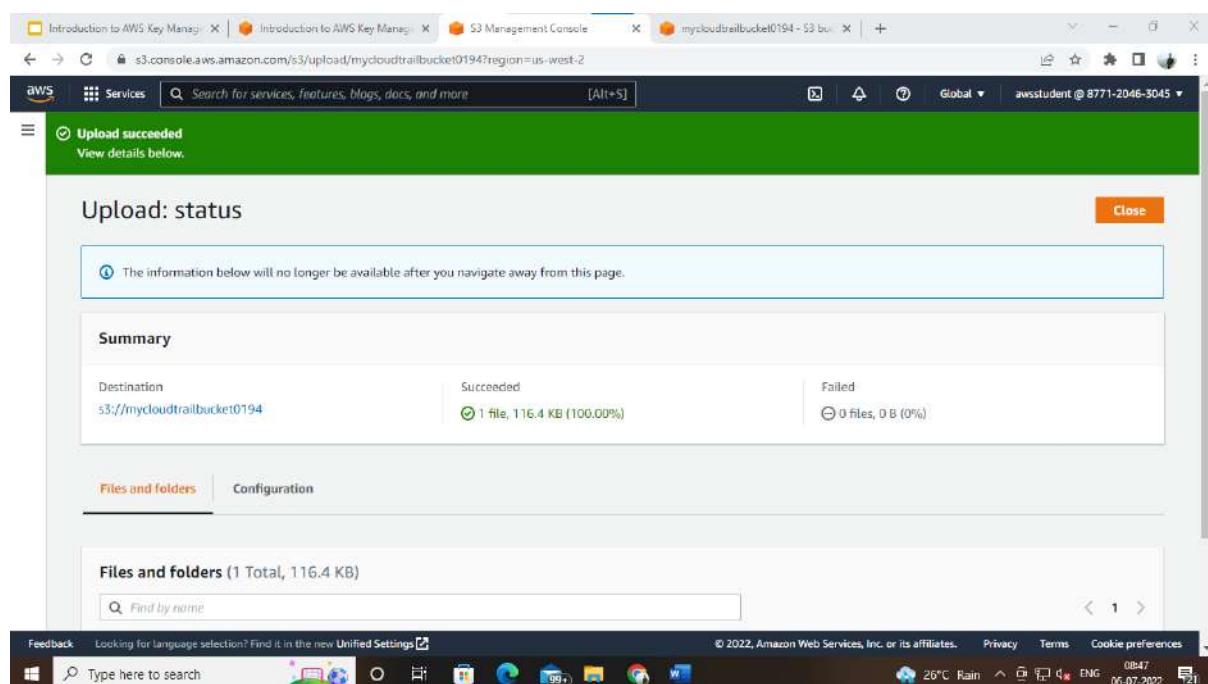


**Step 33 – Form the drop down of the KMS Master key, select *myFirstKey***

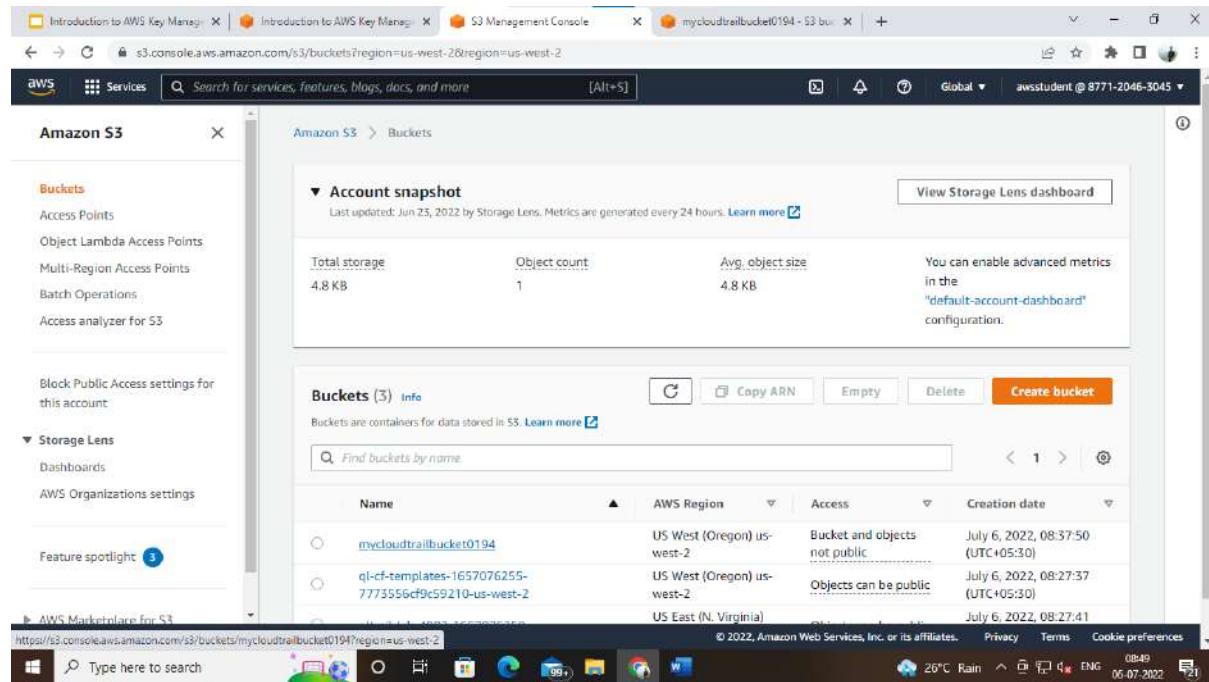
**Step 34 – Scroll to the bottom of the screen, then click Upload.**



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

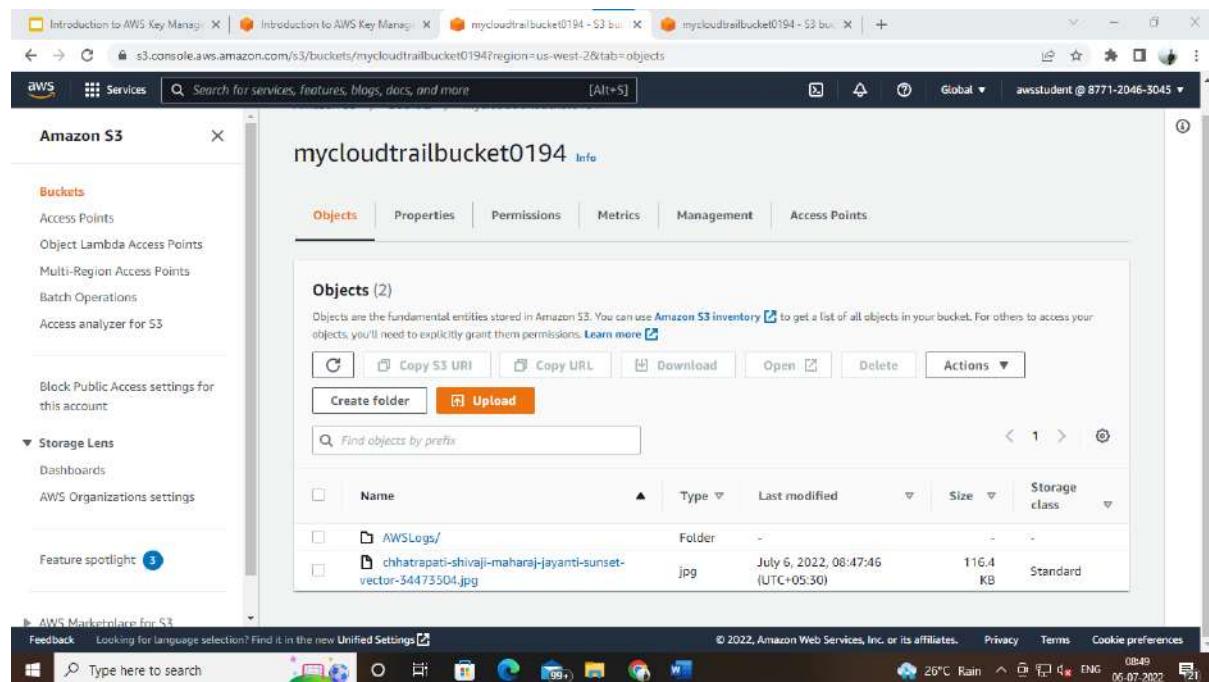


**Step 36 – Return to the bucket details by clicking the bucket name.**



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

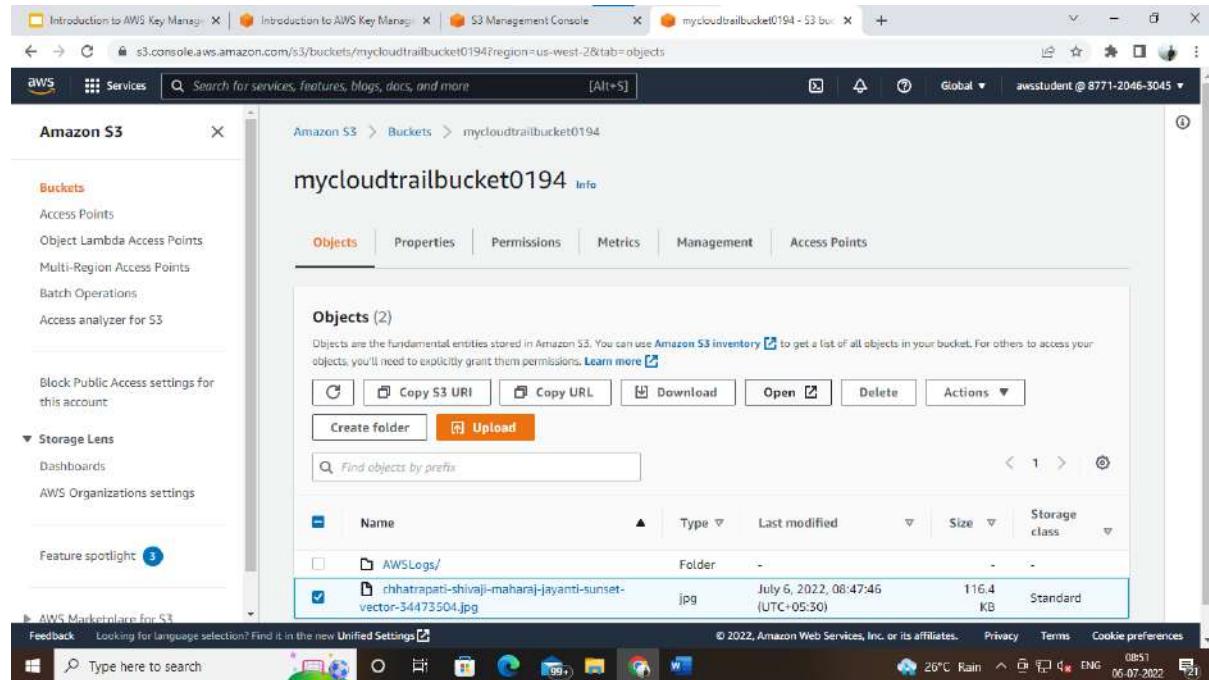
**Step 38 – Return to the bucket details by clicking the bucket name.**



## Task 4: Access the Encrypted Image

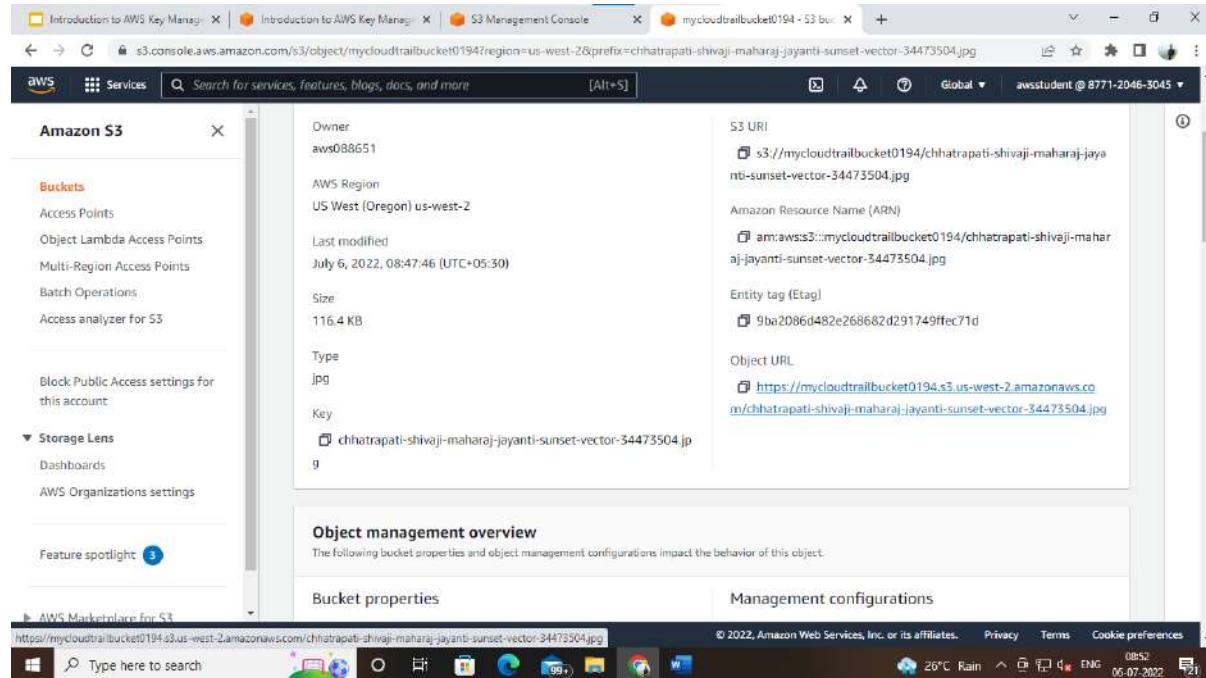
In this task, you will try to access the encrypted image through both the AWS management Console and the S3 link.

**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.

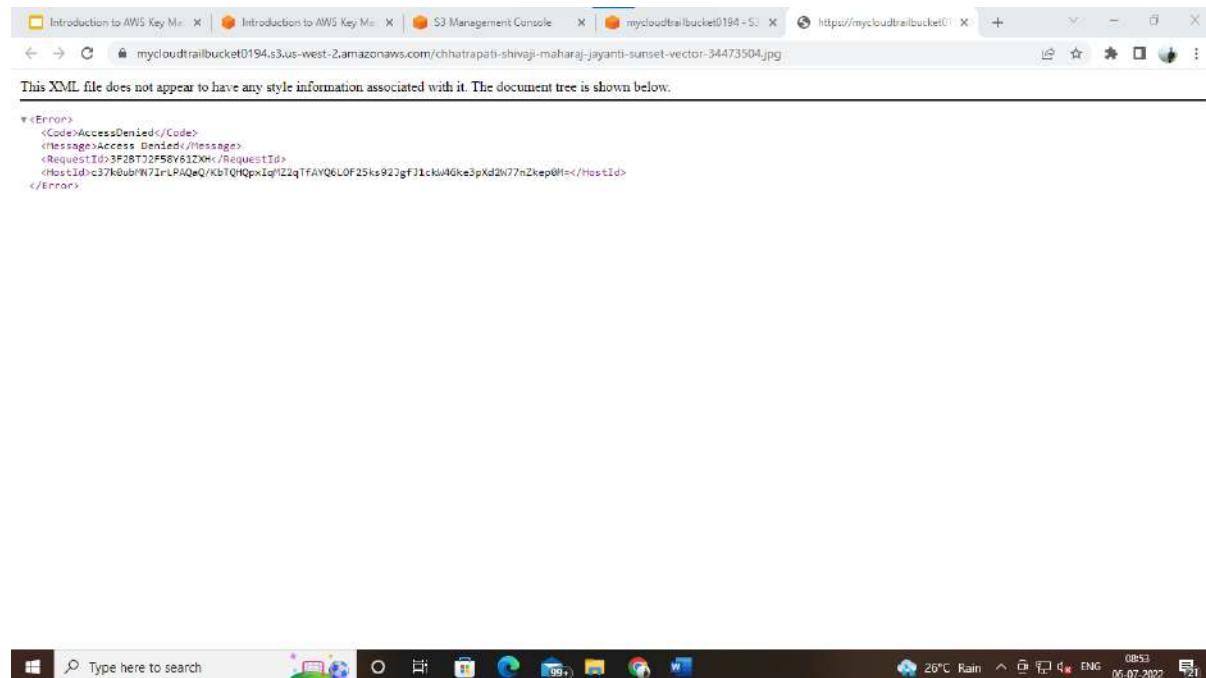


**Step 42 – Paste the S3 object URL that you copied earlier into new browser/window.**

**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.

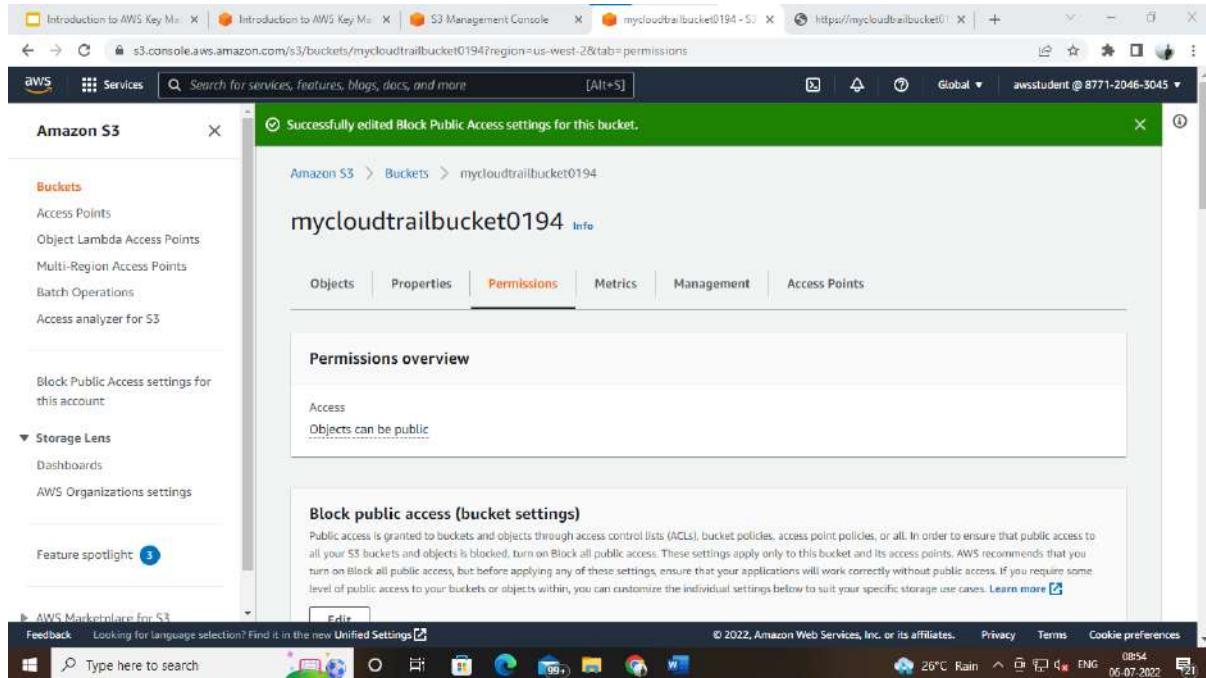
**Step 46 –** Click the Permission tab.

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

## Step 48 – De-select Block all public access.

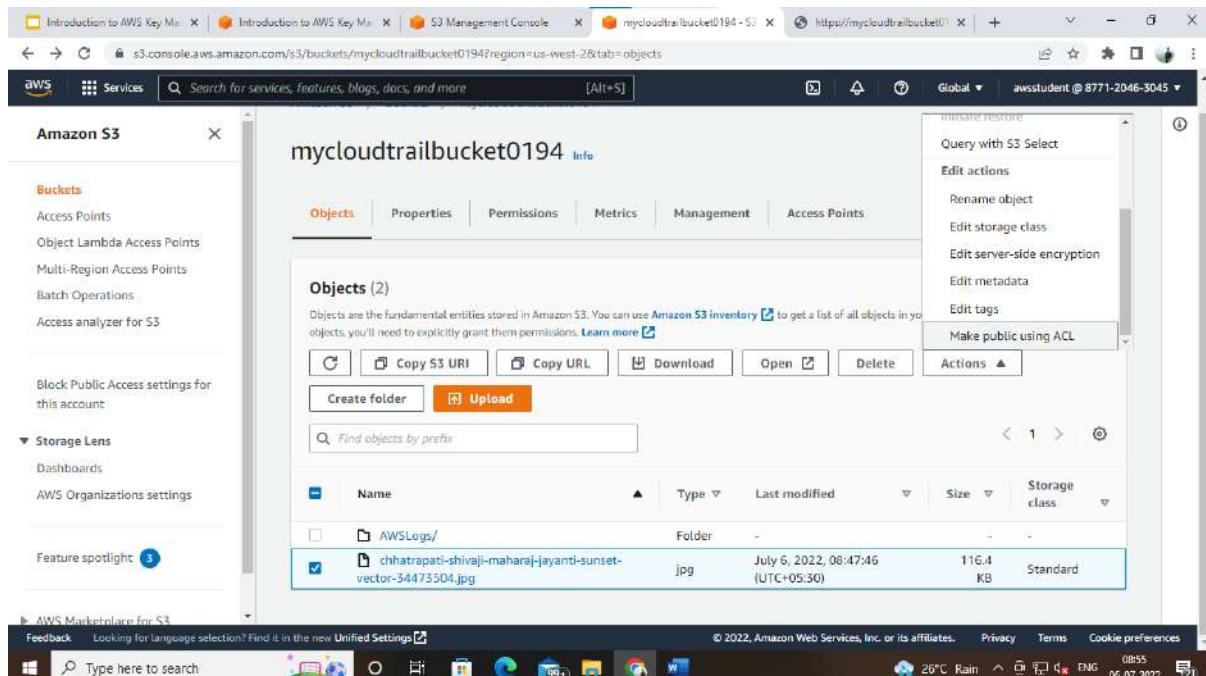
## Step 49 – Click Save changes then:

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

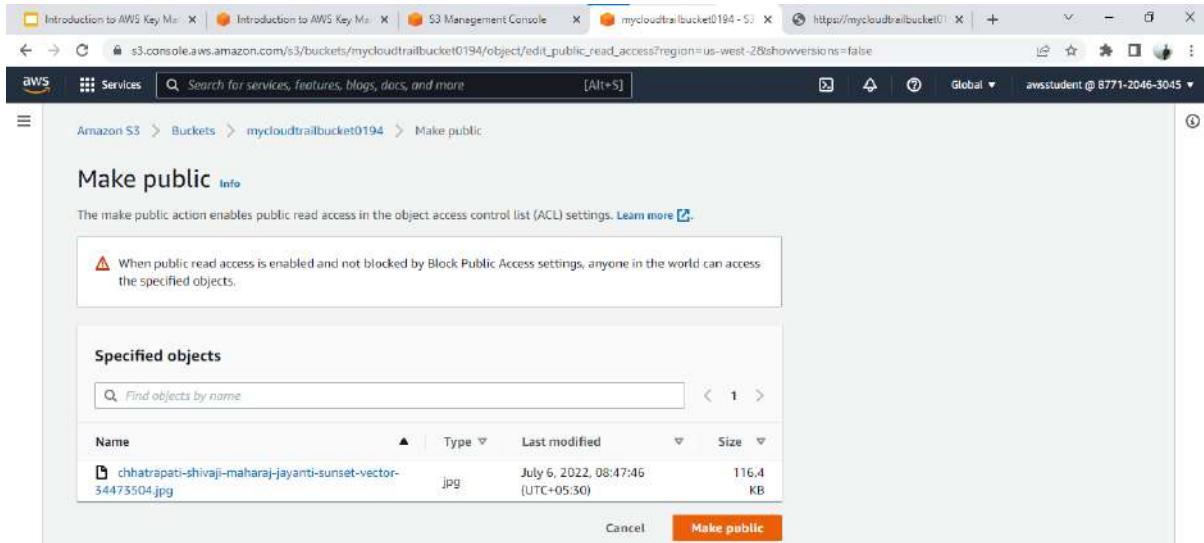


**Step 50 – In the Object tab, Select your image.**

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



**Step 52 – Click Make public.**

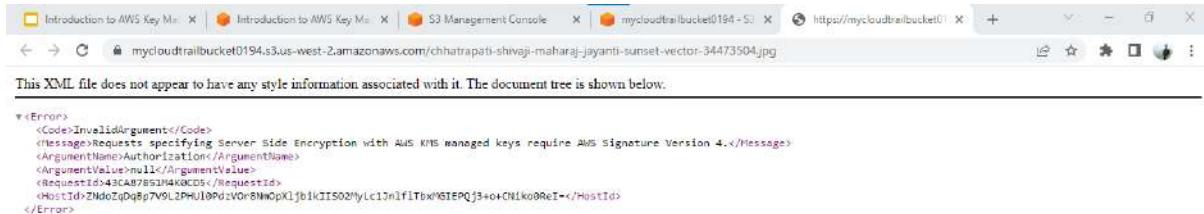


Source	Successfully edited public access	Failed to edit public access
s3://mycloudtrailbucket0194	1 object, 116.4 KB	0 objects

**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.



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0"?>
<Error>
  <Code>InvalidArgument</Code>
  <Message>Requests specifying Server Side Encryption with AWS KMS managed keys require AWS Signature Version 4.</Message>
  <ArgumentName>Authorization</ArgumentName>
  <ArgumentValue>nul</ArgumentValue>
  <RequestId>43CAB7B5-1A4K-4CD5-</RequestId>
  <HostId>ZMdoZqDg8p7V9L2PHU1P9dzVOr8NwOpX1jbikII502MyLc1JnlfITbxW6IEPQj3+o+CNiko0ReI=</HostId>
</Error>
```



**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.**

Amazon S3 > Buckets > mycloudtrailbucket0194

**Objects (2)**

Name	Type	Last modified	Size	Storage class
AWSLogs/	Folder	-	-	-
chhatrapati-shivaji-maharaj-jayanti-sunset-vector-34473504.jpg	jpg	July 6, 2022, 08:47:46 (UTC+05:30)	116.4 KB	Standard

Amazon S3 > Buckets > mycloudtrailbucket0194 > AWSLogs/ > 877120463045/ > CloudTrail/ > us-west-2/ > 2022/ > 07/ > 06/

**Objects (10)**

Name	Type	Last modified	Size	Storage class
877120463045_CloudTrail_us-west-2_20220706T0315Z_Dex1KC8XKWDPhs9T.json.gz	gz	July 6, 2022, 08:47:57 (UTC+05:30)	549.0 B	Standard

**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

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with 'Amazon S3' navigation, including 'Buckets', 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', and 'Access analyzer for S3'. Below that are sections for 'Block Public Access settings for this account', 'Storage Lens', 'Dashboards', 'AWS Organizations settings', and 'Feature spotlight'. The main area displays a table of objects:

Name	Type	Last modified	Size	Storage class
<code>L_20220706105256_VmUQKwZYonyAnsY.json.gz</code>		(UTC+05:30)		
<code>877120463045_CloudTrail_us-west-2_20220706105302_iXBHj5gCERtzIwa5.json.gz</code>	gz	July 6, 2022, 08:58:36 (UTC+05:30)	18.2 KB	Standard
<code>877120463045_CloudTrail_us-west-2_20220706T0330Z_MEv2GqmE0ZyGzah3.json.gz</code>	gz	July 6, 2022, 08:58:35 (UTC+05:30)	10.5 KB	Standard
<code>877120463045_CloudTrail_us-west-2_20220706T0335Z_GuxWjGWjSIyWkQFC.json.gz</code>	gz	July 6, 2022, 09:03:47 (UTC+05:30)	6.9 KB	Standard
<code>877120463045_CloudTrail_us-west-2_20220706T0335Z_pTh1Ex3ef3kMkBEl.json.gz</code>	gz	July 6, 2022, 09:03:45 (UTC+05:30)	8.0 KB	Standard

At the bottom of the table, there are buttons for 'Create folder', 'Upload', and a search bar labeled 'Find objects by prefix'. The status bar at the bottom right shows '26°C Rain', 'ENG', and the date '06-07-2022'.

This screenshot shows the AWS CloudTrail logs page. It displays a single JSON object with many nested fields, representing the CloudTrail log entries. The JSON structure includes fields like 'Records', 'EventVersion', 'UserIdentity', 'EventTime', 'SourceIPAddress', 'RequestParameters', 'ResponseElements', and various AWS-specific parameters. The JSON is very long and contains numerous log entries from different users and accounts.

The status bar at the bottom right shows '26°C Rain', 'ENG', and the date '06-07-2022'.

**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.

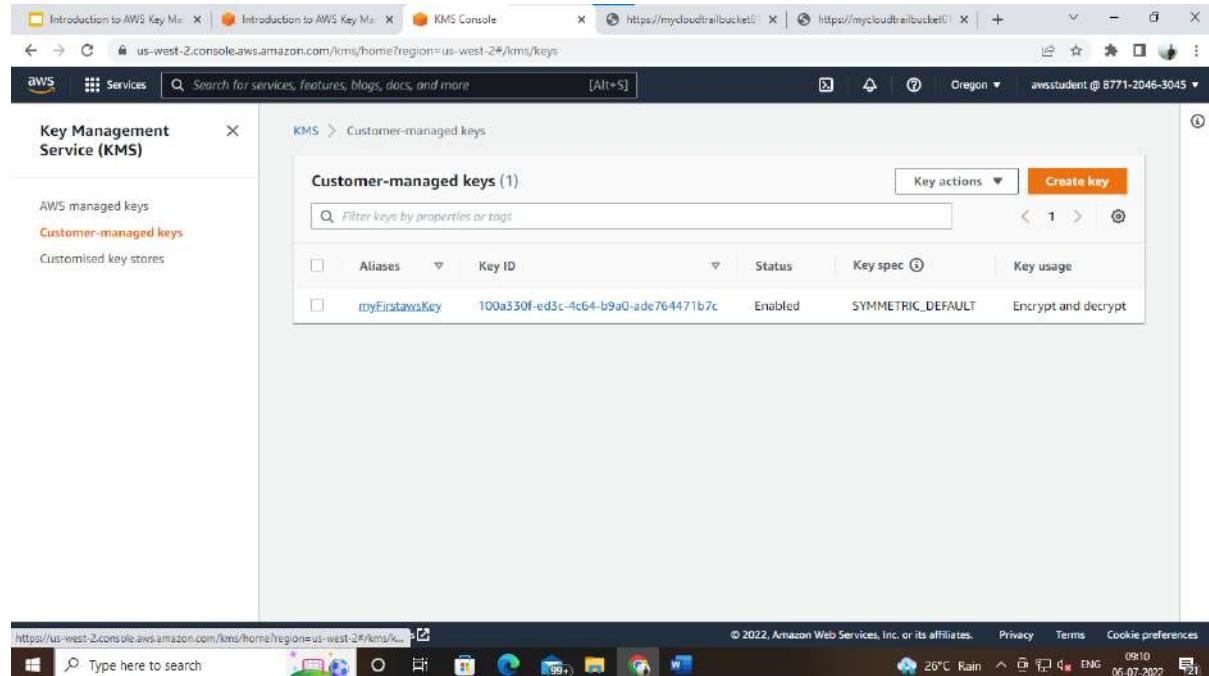
In this task you will manage encryption key for users and role.

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

The screenshot shows the AWS CloudTrail console interface. On the left, there's a sidebar with 'Recently visited' and 'Favorites' sections, and a main area listing various AWS services like S3, CloudTrail, Key Management Service, RDS, EC2, etc. On the right, a detailed view of an S3 bucket is shown. A table lists objects in the bucket, with one row for 'myFirstKey' highlighted. The table columns include 'Last modified', 'Size', and 'Storage class'. The 'myFirstKey' row shows a timestamp of '2022-06-07T03:45:30+05:30', a size of '8.0 KB', and a storage class of 'Standard'.

Last modified	Size	Storage class
2022-06-07T03:45:30+05:30	8.0 KB	Standard

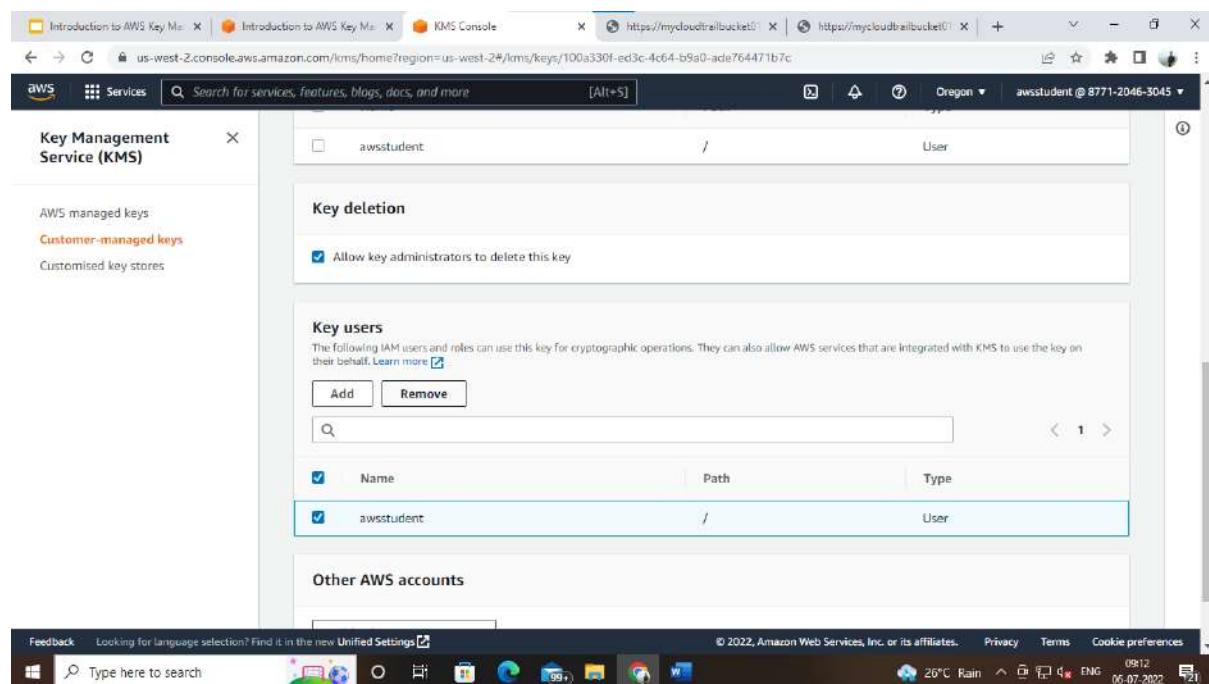
**Step 66** – Click myFirstKey.



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

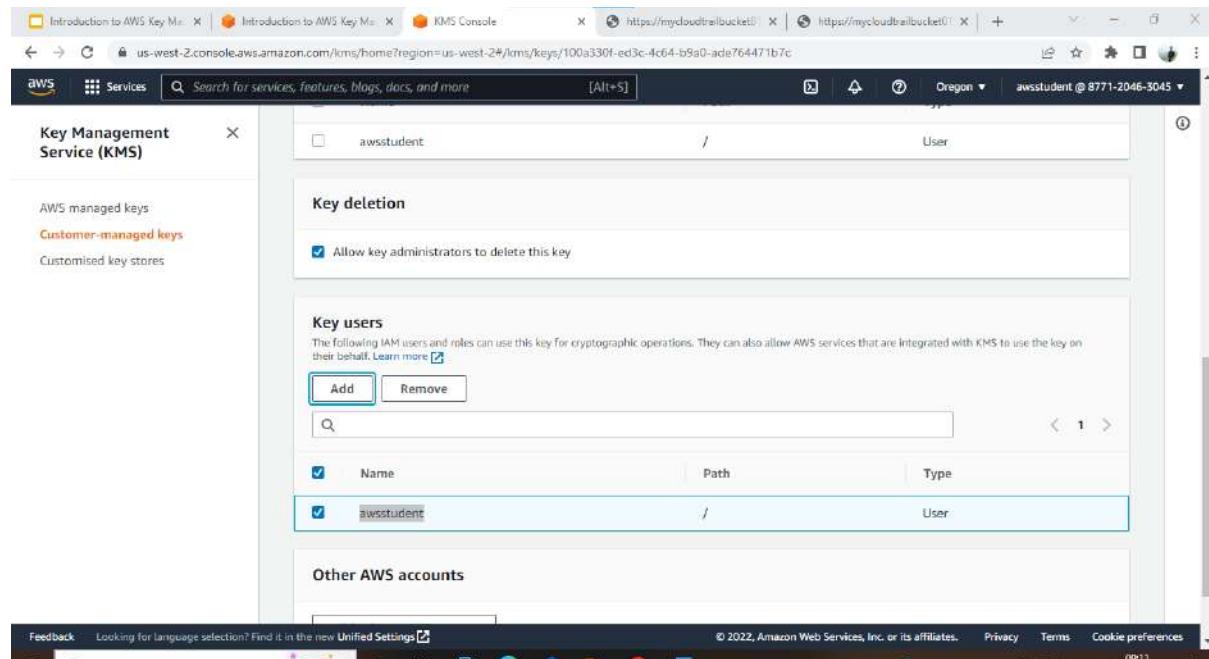
**Step 68** – Click the Remove.

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

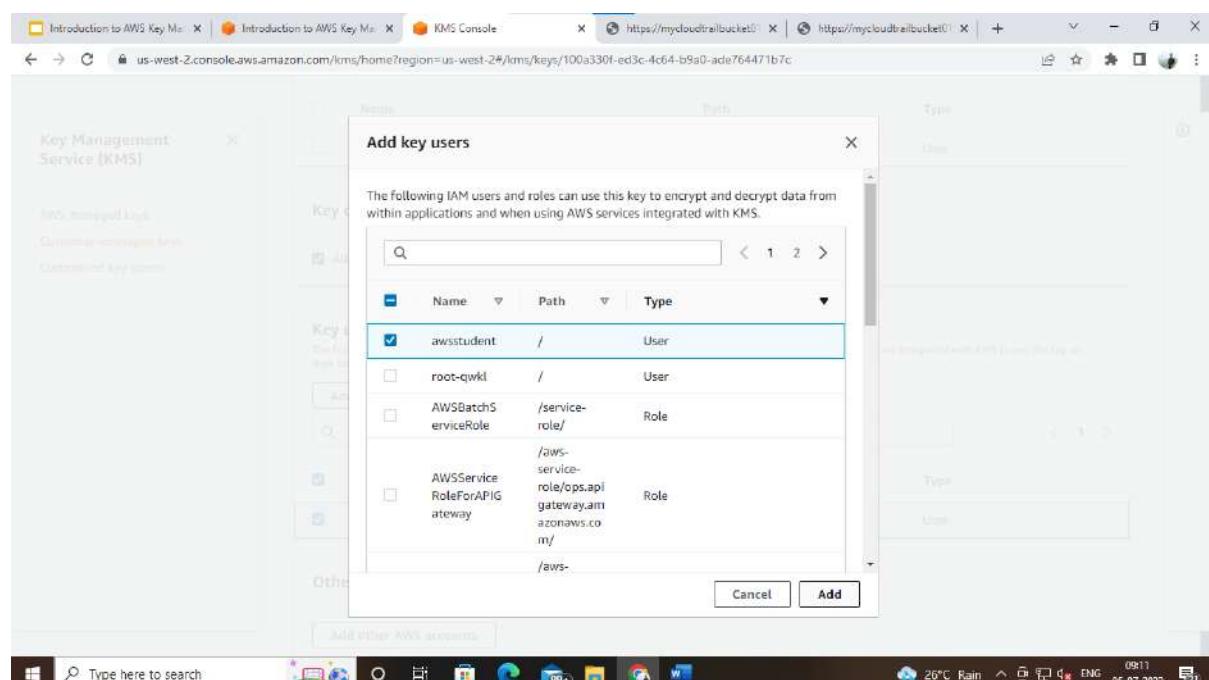


**Step 69 – In the Key user section, Click the Add then:**

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



The screenshot shows the AWS KMS Console interface. On the left, there's a sidebar with 'Key Management Service (KMS)' and links for 'AWS managed keys', 'Customer-managed keys', and 'Customised key stores'. The main area is titled 'Key users' and contains a table with one row for 'awsstudent'. Below the table, there's a section for 'Other AWS accounts' which is currently empty. At the bottom of the page, there's a search bar and a status bar showing the date and time.

This screenshot shows the 'Add key users' dialog box. It lists several IAM users and roles, with 'awsstudent' selected. The 'Add' button at the bottom right is highlighted. The background shows the same KMS console interface as the previous screenshot.

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.

## 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

### Step 1 – Start Lab and click on Open Console

Start Lab 00:45:00

# Introduction to Amazon DynamoDB

45 minutes Free ★★★★  
aws training and certification

SPL-71 - Version 3.0.12

© 2022 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. All trademarks are the property of their owners.

Note: Do not include any personal, identifying, or confidential information into the lab

Lab Overview  
Topics covered  
**Start lab**  
Task 1: Create a New Table  
Task 2: Add Data  
Task 3: Modify an Existing Item  
Task 4: Query the Table  
Task 5: Delete the Table  
End lab  
Conclusion  
Additional Resources

End Lab 00:44:42

## Start lab

1. To launch the lab, at the top of the page, choose **Start Lab**.

This starts the process of provisioning the lab resources. An estimated amount of time to provision the lab resources is displayed. You must wait for the resources to be provisioned before continuing.

💡 If you are prompted for a token, use the one distributed to you (or credits you have purchased).

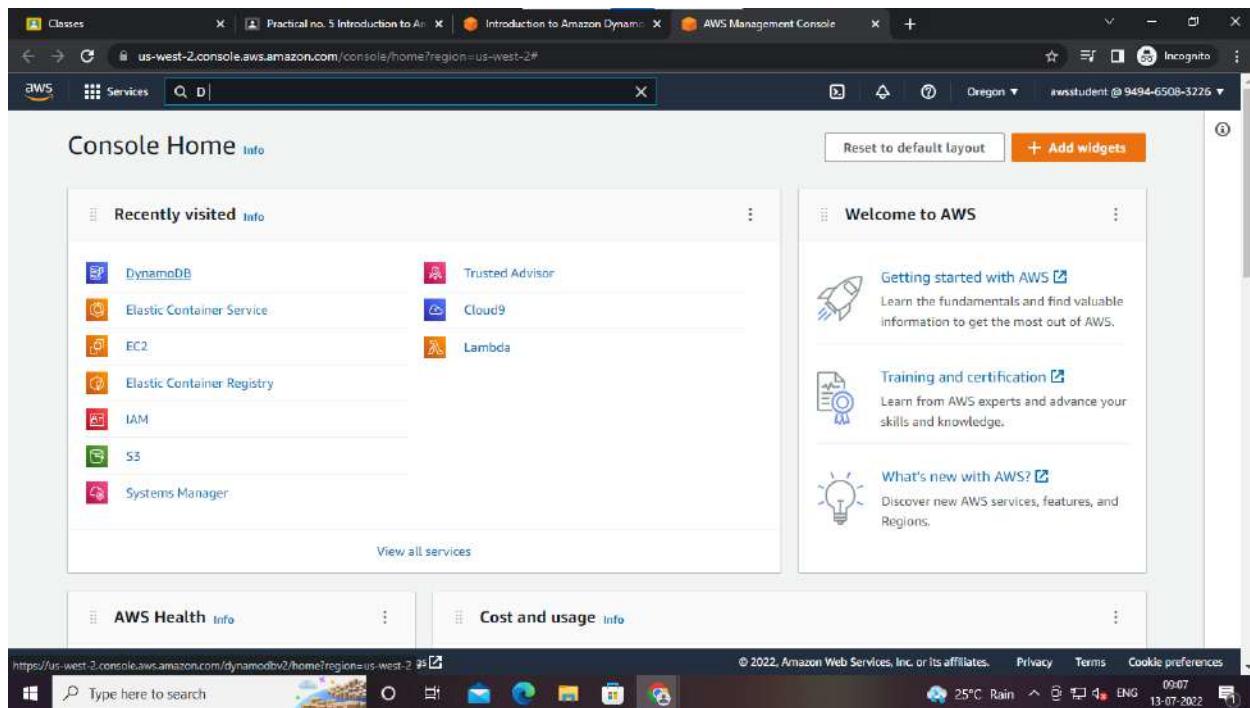
2. To open the lab, choose **Open Console**.

You are automatically signed in to the AWS Management Console in a new web browser tab.

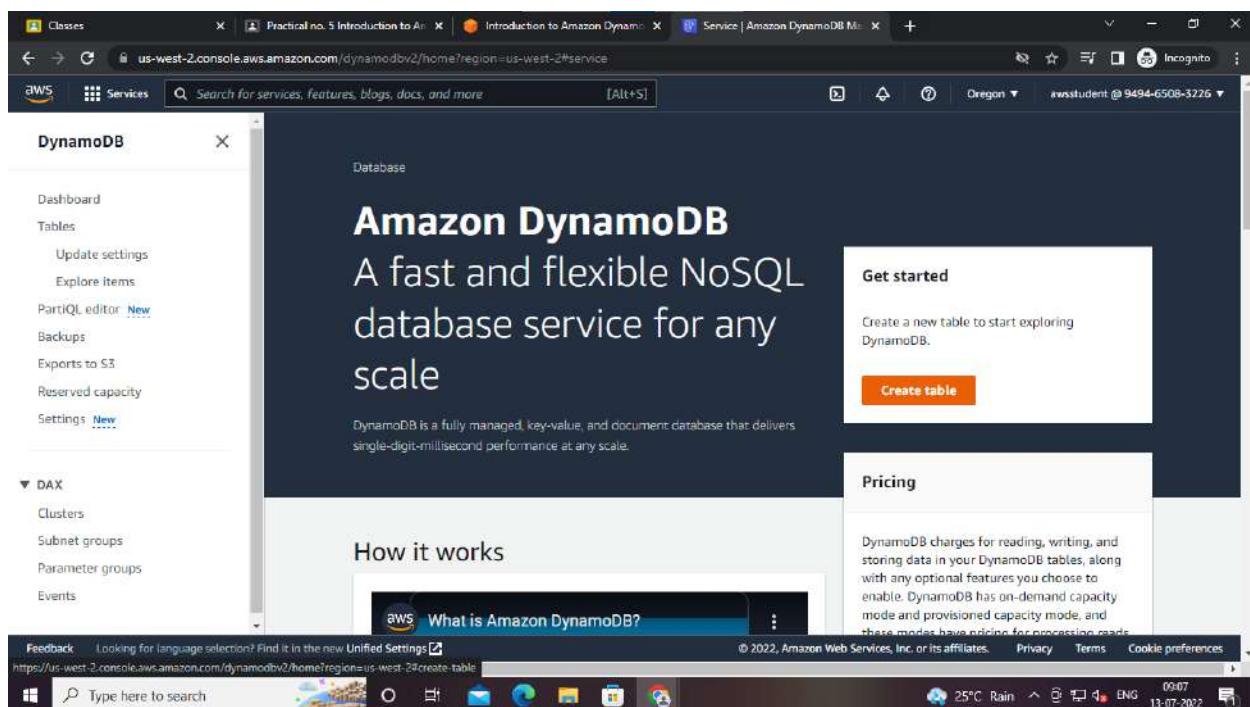
⚠️ Do not change the Region unless instructed.

### Common sign-in errors

### Step 2 – In the AWS Management Console, choose **Services**, 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.

The screenshot shows the 'Create table' wizard in the AWS Management Console. The 'Table details' step is active. The 'Table name' field contains 'Music'. The 'Partition key' field contains 'Artist' with a type of 'String'. The 'Sort key - optional' field contains 'Song' with a type of 'String'. The status bar at the bottom right shows '13-07-2022' and '09:08'.

### Step 7 – Choose Create table.

The table will be created in less than a minute.

The screenshot shows the final configuration screen before creating the table. It includes sections for 'Default settings' (using standard values), 'Tags' (no tags associated), and a note about auto-scaling (disabled due to lack of permissions). The 'Create table' button is visible at the bottom right. The status bar at the bottom right shows '13-07-2022' and '09:08'.

### Step 8 – Wait for your table to be created.

The screenshot shows the AWS DynamoDB console interface. On the left, a sidebar menu includes 'Dashboard', 'Tables' (selected), 'Update settings', 'Explore items', 'PartiQL editor', 'Backups', 'Exports to S3', 'Reserved capacity', and 'Settings'. Under 'Tables', there's a 'DAX' section with 'Clusters', 'Subnet groups', 'Parameter groups', and 'Events'. The main content area displays a table titled 'Tables (1) Info' with one item: 'Music'. The table has columns for 'Name', 'Status', 'Partition key', 'Sort key', 'Indexes', 'Read capacity mode', 'Write capacity mode', and 'Size'. The 'Status' column shows 'Creating'. A message at the top says 'Creating the Music table. It will be available for use shortly.' The bottom of the screen shows a Windows taskbar with various icons and a system status bar indicating '25°C Rain'.

This screenshot is identical to the one above, showing the AWS DynamoDB console. The 'Tables' section is selected in the sidebar. The main table now shows the 'Music' table with its status changed to 'Active'. A warning message at the top states 'Your Music table was created with auto scaling turned off. Try enabling auto scaling from table settings.' The Windows taskbar at the bottom remains the same.

## 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**.

Name	Status	Partition key	Sort key	Indexes	Read capacity mode	Write capacity mode	Size
Music	Active	Artist (S)	Song (S)	0	Provisioned (5)	Provisioned (5)	0 bytes

**Step 10 –** Select **Music**.

**Step 11 –** Choose **Create Item**.

The screenshot shows the AWS DynamoDB console interface. On the left, there's a sidebar with 'DynamoDB' navigation. Under 'Tables', 'Explore items' is selected. In the main content area, a 'Tables (1)' panel shows a single table named 'Music'. Below it, the 'Music' table details are shown with an 'Autopreview' button and a 'View table details' link. A 'Scan/Query items' section indicates 'Items returned (0)' and displays the message 'The query did not return any results.' The browser address bar shows the URL for the 'Edit item' page.

**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.

The screenshot shows the 'Edit item' page for the 'Music' table. The top navigation bar includes 'Edit item | Amazon DynamoDB'. The main form has 'Form' and 'JSON' tabs. The 'Attributes' section contains two entries:

Attribute name	Value	Type
Artist - Partition key	Pink Floyd	String
Song - Sort key	Money	String

At the bottom right are 'Cancel' and 'Create Item' buttons. The browser address bar shows the URL for the 'Edit item' page.

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

The screenshot shows the AWS Lambda function configuration page. The 'Handler' field is highlighted with a red box. The code in the Handler field is:

```
function(event, context) {
    const response = {
        statusCode: 200,
        body: JSON.stringify({
            message: 'Hello from Lambda'
        })
    };
    context.succeed(response);
}
```

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

The screenshot shows the AWS Lambda function configuration page. The 'Handler' field is highlighted with a red box. The code in the Handler field is:

```
function(event, context) {
    const response = {
        statusCode: 200,
        body: JSON.stringify({
            message: 'Hello from Lambda'
        })
    };
    context.succeed(response);
}
```

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

The screenshot shows the 'Edit item' screen in the AWS Lambda console. The URL is <https://us-west-2.console.aws.amazon.com/dynamodbv2/home?region=us-west-2#edit-item?table=Music&ref=%23item-explorer%3Ftable%3DMusic&route=ROUT...>. The page title is 'Edit item | Amazon DynamoDB'. The navigation path is 'DynamoDB > Items: Music > Edit item'. There are two tabs at the top right: 'Form' (selected) and 'JSON'.  
  
The main area is titled 'Create item' with the sub-instruction: 'You can add, remove, or edit the attributes of an item. You can nest attributes inside other attributes up to 32 levels deep. [Learn more](#)'.  
  
A table titled 'Attributes' lists three items:

Attribute name	Value	Type
Artist - Partition key	Pink Floyd	String
Song - Sort key	Money	String
Album	The Dark Side of the Moon	String

  
At the bottom right are 'Cancel' and 'Create item' buttons.

**Step 17 – Add another new attribute.**

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

The screenshot shows the AWS DynamoDB console with the 'Create item' form. A context menu is open over the 'Type' column for the 'Album' attribute, listing various data types: String, Number, Boolean, Binary, Null, String set, Number set, Binary set, List, and Map. The 'String' option is currently selected.

Attribute name	Value	Type
Artist - Partition key	Pink Floyd	String
Song - Sort key	Money	String
Album	The Dark Side of the Moon	String

A new number attribute will be added.

**Step 18 – For the new attribute, enter:**

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

The screenshot shows the AWS DynamoDB console with the 'Create item' form. A new attribute 'Year' has been added with a value of 1973 and a type of Number. The 'Create Item' button is visible at the bottom right.

Attribute name	Value	Type
Artist - Partition key	Pink Floyd	String
Song - Sort key	Money	String
Album	The Dark Side of the Moon	String
Year	1973	Number

**Step 19 – Choose Save changes.**

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

The screenshot shows the 'Edit item' page for a DynamoDB table named 'Music'. The 'Attributes' section contains the following data:

Attribute name	Value	Type
Artist - Partition key	Pink Floyd	String
Song - Sort key	Money	String
Album	The Dark Side of the Moon	String
Year	1973	Number

At the bottom right, there are 'Cancel' and 'Create item' buttons. The 'Create item' button is highlighted in orange.

The item will appear in the console.

The screenshot shows the 'Items' page for the 'Music' table. A green success message at the top left states: 'The item has been saved successfully.' The 'Tables (1)' sidebar shows one table named 'Music'. The main 'Music' section displays the following data in the 'Items returned' table:

Artist	Song	Album	Year
John Lennon	Imagine	Imagine	1971
Pink Floyd	Money	The Dark Si...	1973

At the bottom right, there are 'Actions' and 'Create item' buttons.

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

Attribute name	Value	Type
Song - Sort key	Imagine	String
Album	Imagine	String
Year	1971	Number
Genre	Soft rock	String

**Create item**

You can add, remove, or edit the attributes of an item. You can nest attributes inside other attributes up to 32 levels deep. Learn more [?](#)

Add new attribute ▾

Cancel Create item

Note that 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.

The item has been saved successfully.

**DynamoDB**

- Dashboard
- Tables
  - Update settings
  - Explore items**
- PartiQL editor [New](#)
- Backups
- Exports to S3
- Reserved capacity
- Settings [New](#)

**Tables (1)**

Any table tag

Find tables by table name

**Music**

Autopreview View table details

**Scan/Query items**

Items returned (2)

Artist	Song	Album	Year
John Lennon	Imagine	Imagine	1971
Pink Floyd	Money	The Dark Si...	1973

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

Attribute name	Value	Type
Song - Sort key	Gangnam Style	String
Album	Psy 6 (Six Rules), Part 1	String
Year	2011	Number
LengthSeconds	219	Number

The item has been saved successfully.

Artist	Song	Album	Genre
Psy	Gangnam Style	Psy 6 (Six R...	
John Lennon	Imagine	Imagine	Soft rock
Pink Floyd	Money	The Dark Si...	

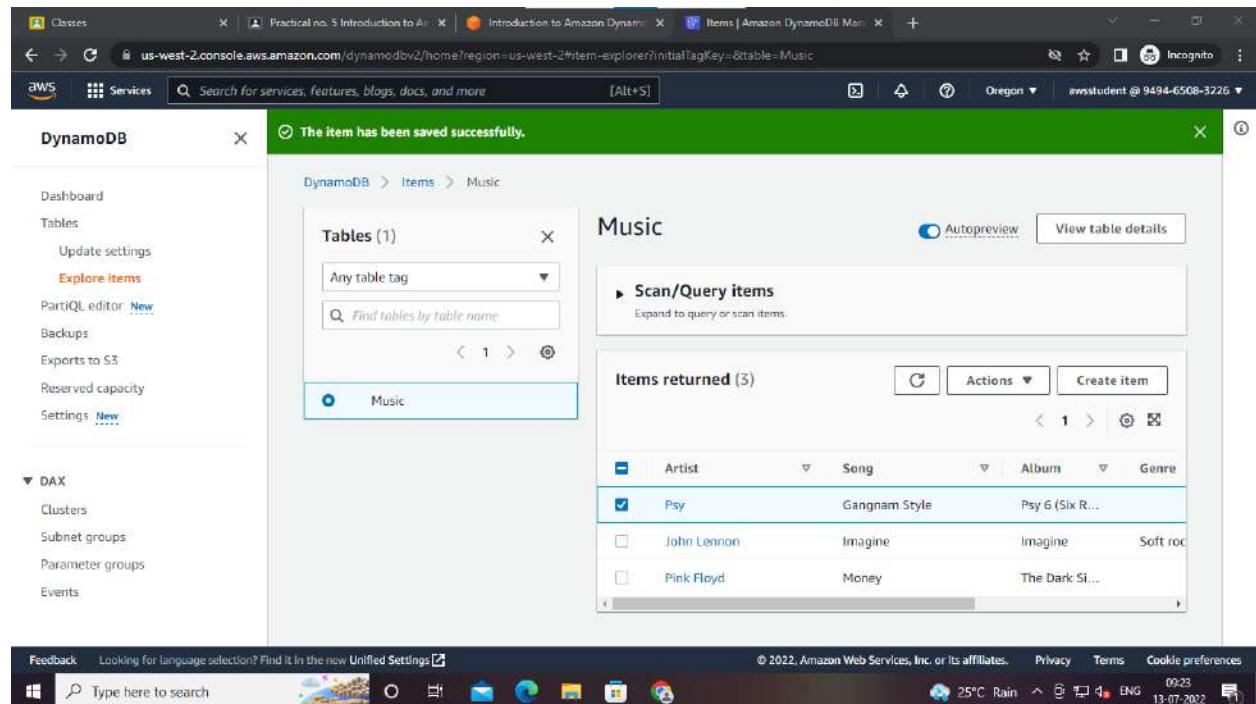
Once again, this item has a new Length Seconds attribute identifying the length of the song. This demonstrates the flexibility of a NoSQL database.

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.



The screenshot shows the AWS DynamoDB Items page for the 'Music' table. A success message at the top says 'The item has been saved successfully.' The table has three items:

Artist	Song	Album	Genre
Psy	Gangnam Style	Psy G (Six R...)	
John Lennon	Imagine	Imagine	Soft rock
Pink Floyd	Money	The Dark Si...	

#### Step 24 – Change the Year from 2011 to 2012.

Attribute name	Value	Type
Song - Sort key	Gangnam Style	New String
Album	Psy 6 (Six Rules), Part 1	String
LengthSeconds	219	Number
Year	2012	Number

## Step 25 – Choose Save changes.

Artist	Song	Album	Genre	LengthSeconds	Year
Psy	Gangnam Style	Psy 6 (Six R...		219	2012
John Lennon	Imagine	Imagine	Soft rock		1971
Pink Floyd	Money	The Dark Si...		219	1973

The item is now updated.

The screenshot shows the AWS DynamoDB console with the 'Music' table selected. The table contains the following data:

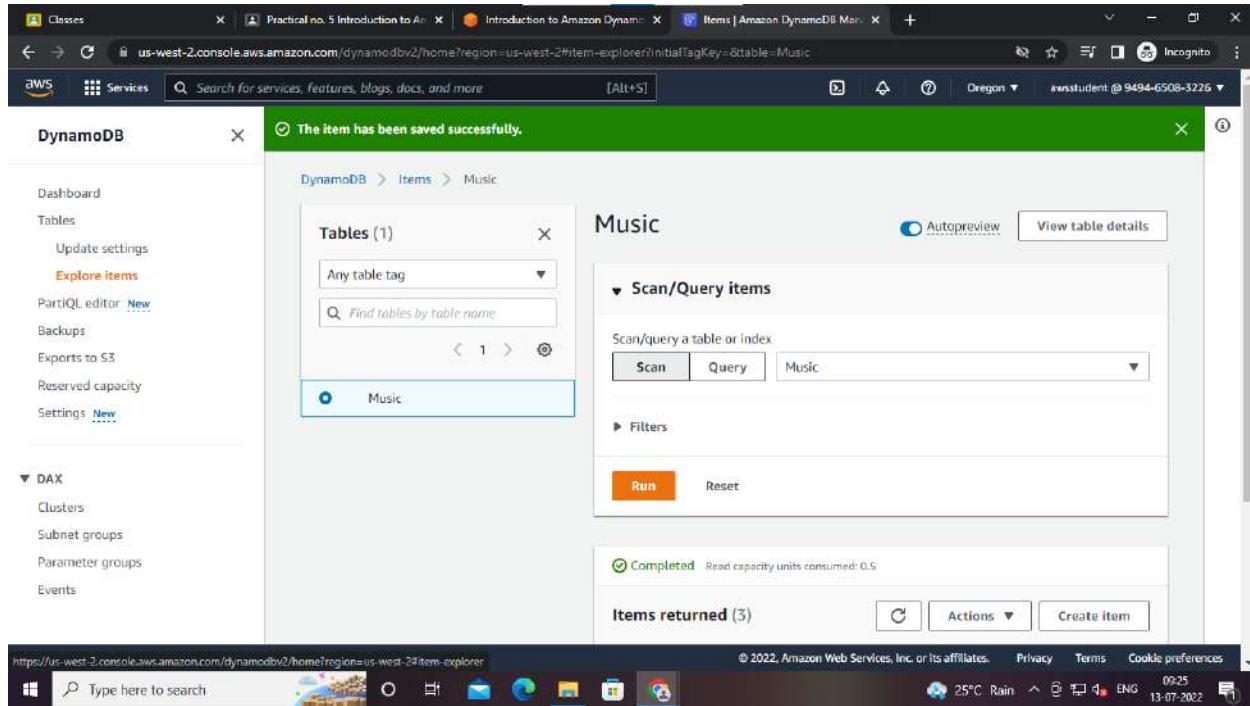
Artist	Song	Album	Genre	LengthSeconds	Year
Psy	Gangnam Style	Psy 6 (Six R...)		219	2012
John Lennon	Imagine	Imagine	Soft rock		1971
Pink Floyd	Money	The Dark Si...			1973

## 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**.

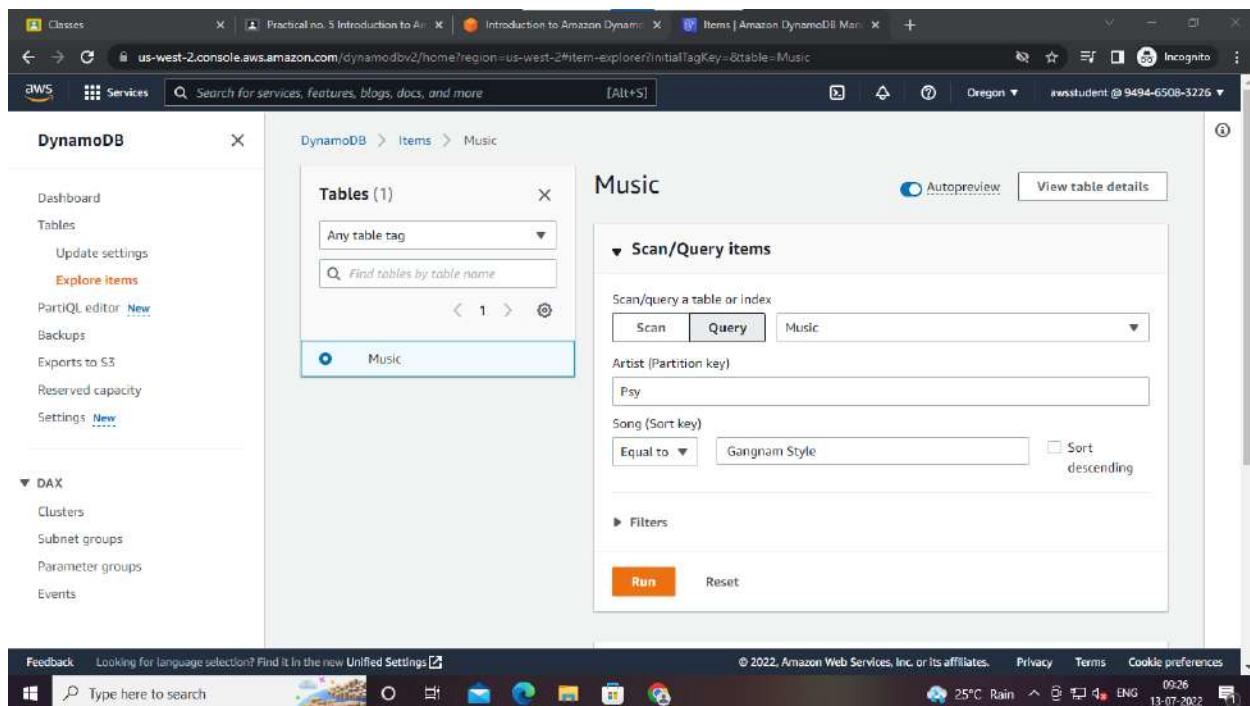


### Step 27 – Choose Music.

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**

The screenshot shows the AWS DynamoDB Items page for the 'Music' table. The left sidebar shows the 'DynamoDB' service with various options like Dashboard, Tables, and Explore items. The main area shows the 'Tables (1)' list with 'Music' selected. On the right, the 'Scan/Query items' section is active, with 'Artist (Partition key)' set to 'Psy' and 'Song (Sort key)' set to 'Gangnam Style' (with 'Equal to' selected). Below these, there's a 'Filters' section and a 'Run' button. The status bar at the bottom indicates 'Completed' with 'Read capacity units consumed: 0.5'.

**Step 31 – Choose Run.**

The screenshot shows the results of the query from Step 30. The 'Items returned (1)' section displays a single item: 'Artist': 'Psy', 'Song': 'Gangnam Style', 'Album': 'Psy G (Six R...', 'Length': '219'. The 'Run' button is highlighted in orange. The status bar at the bottom indicates 'Completed' with 'Read capacity units consumed: 0.5'.

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.

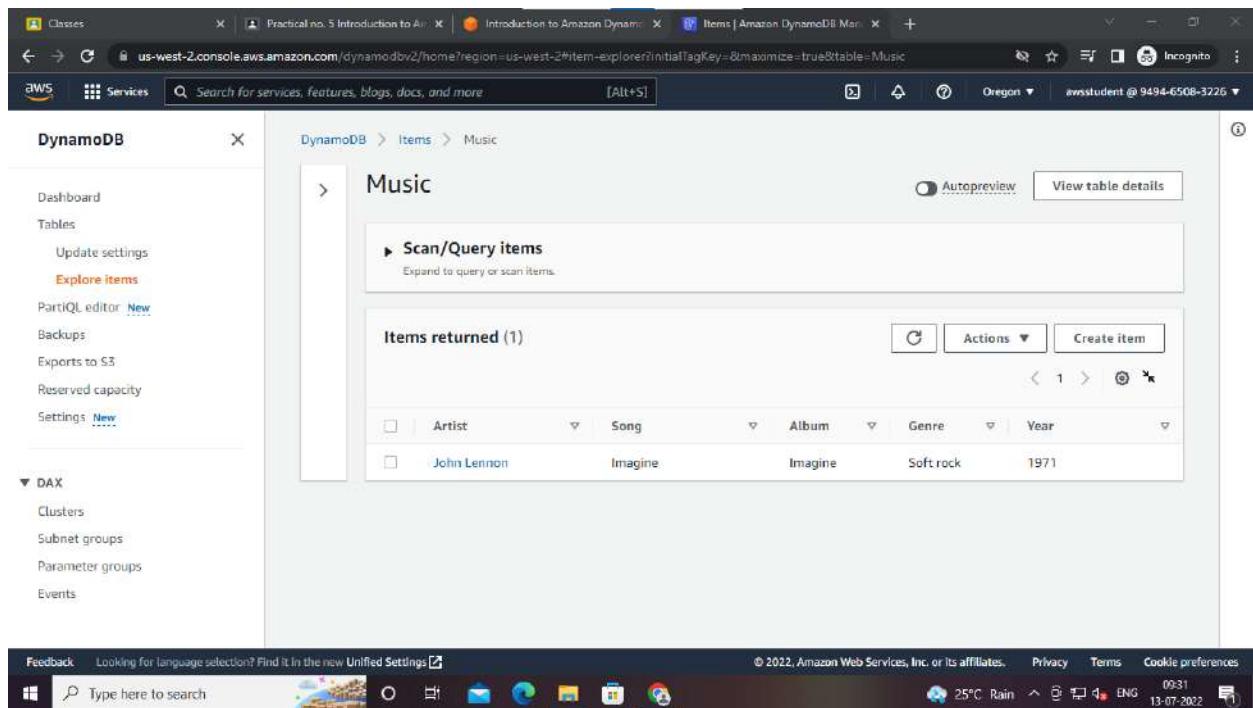
**Step 32** – Choose Scan, then expand the filters, then use this filter.

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

The screenshot shows the AWS DynamoDB Items page for the 'Music' table. On the left, the navigation bar includes 'Dashboard', 'Tables', 'Update settings', 'Explore items' (which is selected), 'PartiQL editor', 'Backups', 'Exports to S3', 'Reserved capacity', and 'Settings'. Below that is a 'DAX' section with 'Clusters', 'Subnet groups', 'Parameter groups', and 'Events'. The main area shows a 'Tables (1)' list with 'Music' selected. To the right, the 'Music' table details are shown with an 'Autopreview' button and a 'View table details' link. Under the 'Scan/Query items' section, the 'Scan' tab is selected, and the 'Music' table is chosen. In the 'Filters' section, there is one filter applied: 'Attribute name: Year', 'Type: Number', 'Condition: Equal to', and 'Value: 1971'. At the bottom, there are 'Add filter' and 'Remove' buttons. The status bar at the bottom indicates 'Feedback' and '© 2022, Amazon Web Services, Inc. or its affiliates.', along with system icons for search, file, mail, and browser.

**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.**

The screenshot shows the AWS DynamoDB console with the URL <https://us-west-2.console.aws.amazon.com/dynamodbv2/home?region=us-west-2#tables>. The left sidebar is collapsed. The main area displays a table titled 'Tables (1) Info'. The table has one row for a table named 'Music'. The columns are: Name, Status, Partition key, Sort key, Indexes, Read capacity mode, Write capacity mode, and Size. The 'Music' table is listed with the following details: Status: Active, Partition key: Artist (S), Sort key: Song (S), Indexes: 0, Read capacity mode: Provisioned (5), Write capacity mode: Provisioned (5), and Size: 0 bytes.

### Step 35 – Choose the Music Tables.

This screenshot is identical to the previous one, but the 'Music' table is now selected, as indicated by a checked checkbox in the first column of the table list. The rest of the interface and table data remain the same.

### Step 36 – Choose Delete.

The screenshot shows the AWS DynamoDB console. On the left, a sidebar menu includes 'Dashboard', 'Tables' (selected), 'Update settings', 'Explore items', 'PartiQL editor', 'Backups', 'Exports to S3', 'Reserved capacity', and 'Settings'. Under 'Tables', there is a 'DAX' section with 'Clusters', 'Subnet groups', 'Parameter groups', and 'Events'. The main content area displays a table titled 'Tables (1) Info'. It shows one table named 'Music' with the following details: Status: Active, Partition key: Artist (\$), Sort key: Song (\$), Indexes: 0, Read capacity mode: Provisioned (5), Write capacity mode: Provisioned (5), and Size: 0 bytes. Below the table is a search bar with placeholder 'Find tables by table name' and a dropdown for 'Any table tag'. At the top right of the main area are buttons for 'Actions', 'Delete', and 'Create table'. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray indicating '25°C Rain'.

**Step 37 – Enter delete.**

**Step 38 – Choose delete table.**

This screenshot shows the same AWS DynamoDB interface as the previous one, but with a modal dialog box in the foreground. The dialog is titled 'Delete table' and contains the message: 'You are about to delete a table.' followed by a list item 'Music'. It has two checkboxes: 'Delete all CloudWatch alarms for this table.' (which is checked) and 'Create a backup of this table before deleting it.' (unchecked). Below the checkboxes is a note: 'If you do not select this check box, you will not be able to restore data being deleted.' At the bottom of the dialog is a text input field containing the word 'delete' and a note: 'To confirm the deletion of this table, type delete in the box.' There are 'Cancel' and 'Delete table' buttons at the bottom right. The background of the window shows the successful deletion message: 'The request to delete the "Music" table has been submitted successfully.'

The table will be deleted.

The screenshot shows the AWS DynamoDB console interface. On the left, there is a navigation sidebar with links for Dashboard, Tables (which is selected), Update settings, Explore items, PartiQL editor, Backups, Exports to S3, Reserved capacity, and Settings. Below these are sections for DAX, Clusters, Subnet groups, Parameter groups, and Events. The main content area is titled "Tables (1) Info" and shows a table with one row. The table has columns for Name, Status, Partition key, Sort key, Indexes, Read capacity mode, Write capacity mode, and Size. The single row is for a table named "Music". The "Status" column shows a red warning icon followed by "Deleting". The "Read capacity mode" and "Write capacity mode" columns both show "Provisioned (5)". The "Size" column shows "0 by". At the top of the main area, a green banner displays the message "The request to delete the "Music" table has been submitted successfully." Below the table, there are buttons for Actions, Delete, and Create table. The browser's address bar shows the URL "us-west-2.console.aws.amazon.com/dynamodbv2/home?region=us-west-2#tables". The bottom of the screen shows the Windows taskbar with various pinned icons and system status information.

## 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

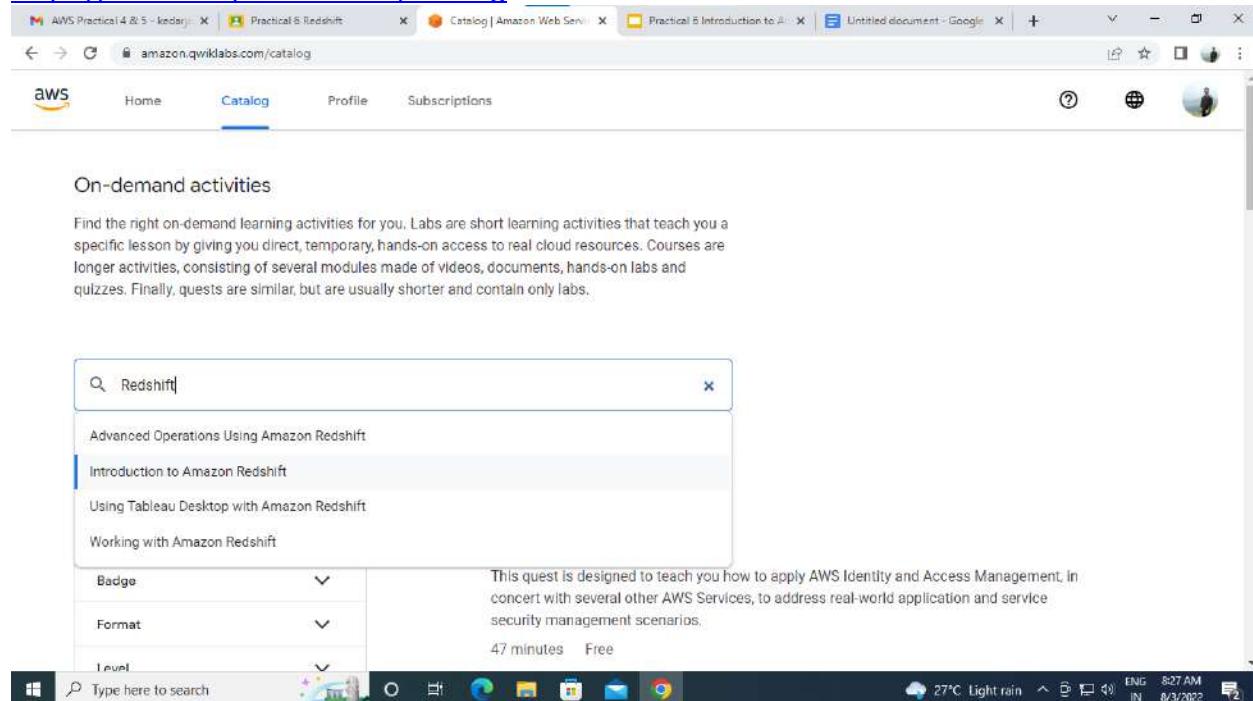
Amazon Redshift is a fast, fully managed data warehouse that makes it simple and cost-effective to analyze all your data using standard SQL and your existing Business Intelligence (BI) tools. It demonstrates the basic steps required to get started with Redshift including:

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>

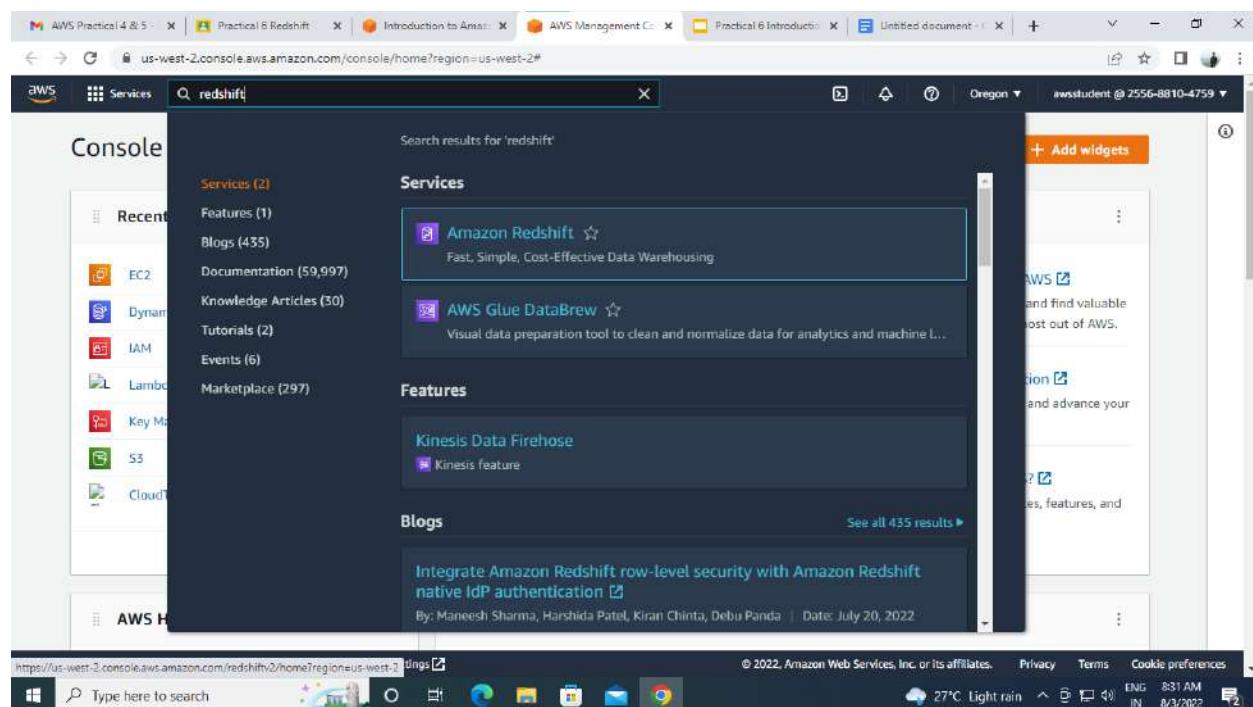


Step 2 – Search the Redshift on given search box, after that show some option then select the “Introduction to Amazon Redshift” same like the below image

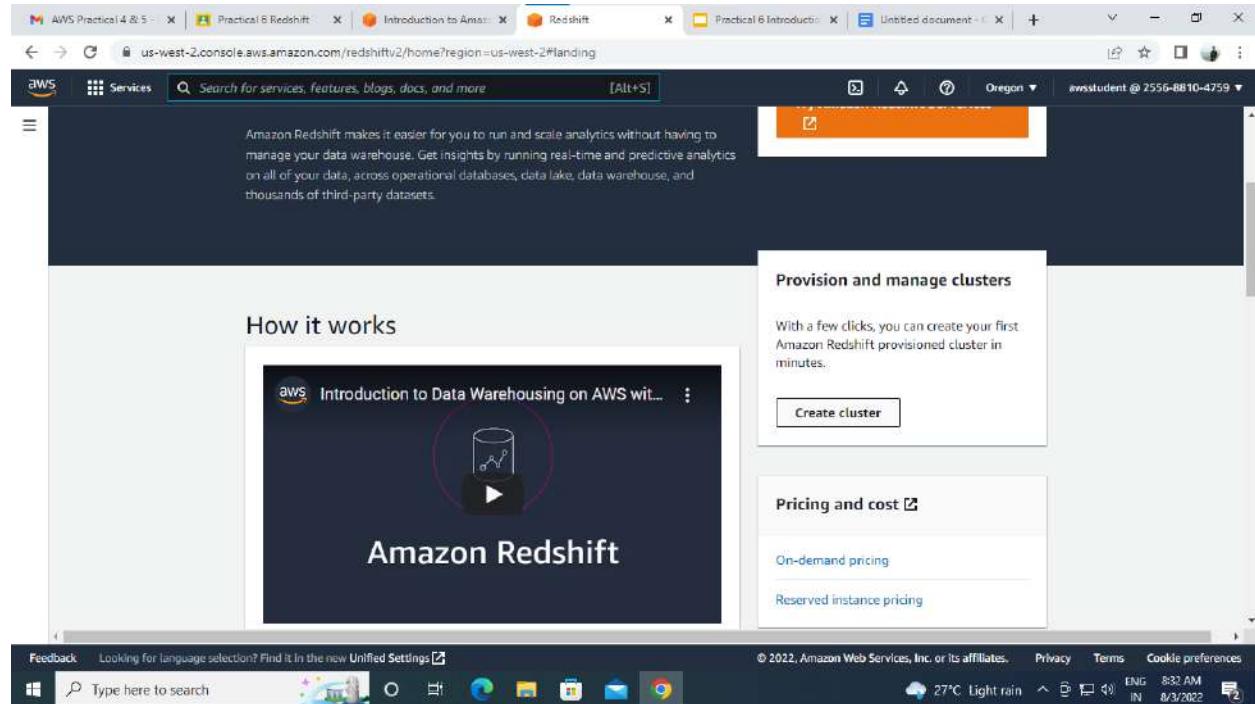
### Step 3 – Start Lab and click on Open Console



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

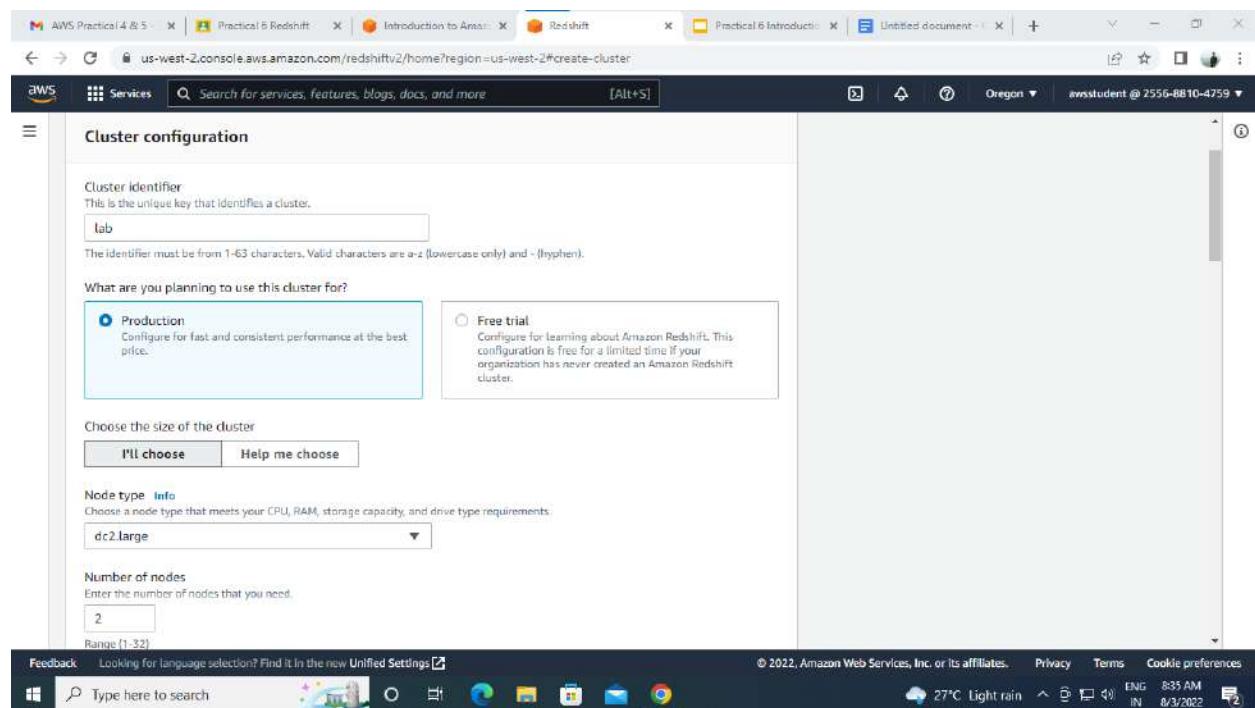


**Step 5 – Choose Create cluster.**



### Step 6 – In the Cluster configuration section, configure:

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

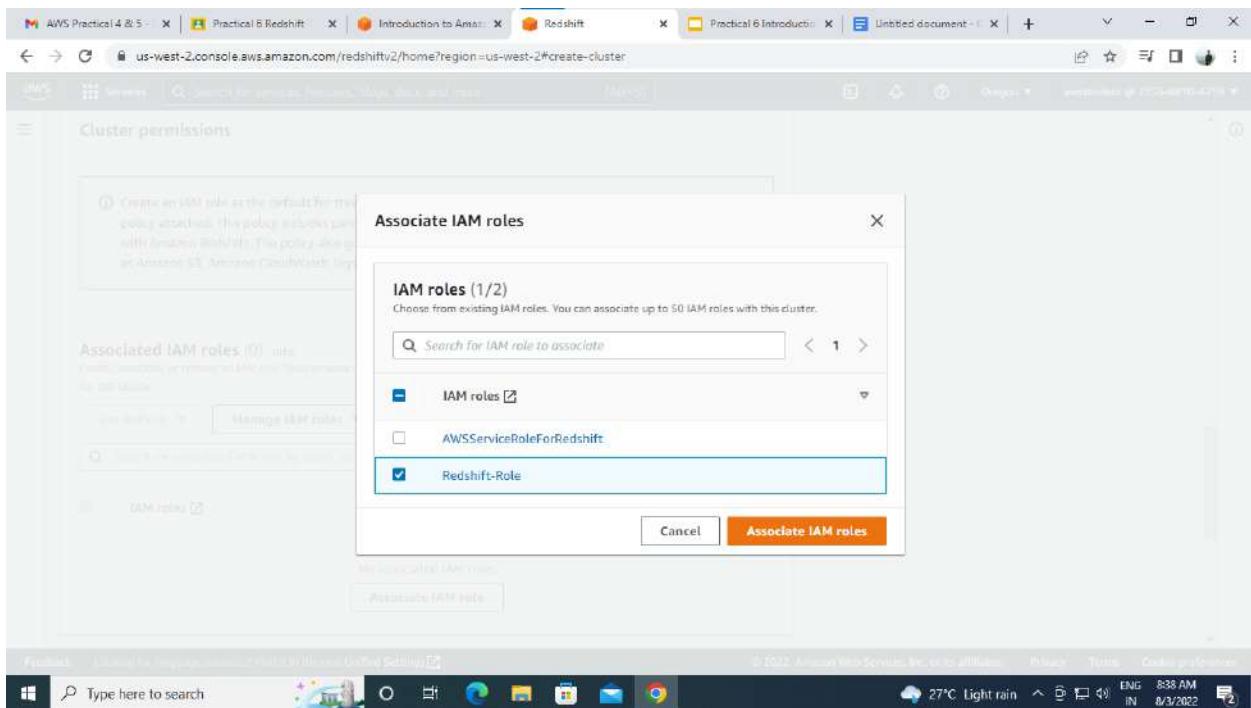


**Step 7 – In the Database configurations section, configure:**

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

The screenshot shows the 'Create Cluster' wizard in the AWS Management Console. The current step is 'Database configurations'. The 'Admin user name' field is set to 'master'. The 'Admin user password' field is set to 'Redshift123'. The 'Show password' checkbox is checked. Below the configuration fields, there is a 'Cluster permissions' section which is currently empty.

**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 default
  - Select Redshift Security Group.

The screenshot shows the AWS IAM Roles page. A specific role named "Redshift-Role" is selected. The interface includes a search bar, filters for IAM roles, status, and role type, and a table listing the selected role.

**Additional configurations** (Use defaults)

These configurations are optional, and default settings have been defined to help you get started with your cluster. Turn off "Use defaults" to modify these settings now.

- Network and security
- Database configurations
- Maintenance
- Monitoring

Feedback Looking for language selection? Find it in the new Unified Settings [?](#)

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Windows taskbar: Type here to search, 27°C Light rain, ENG 8:42 AM IN 8/3/2022

The screenshot shows the AWS VPC configuration page for a Redshift cluster. It displays the selected VPC ("Lab VPC") and a note that the VPC cannot be changed after cluster creation. It also shows the default VPC security group ("default") selected.

**Additional configurations** (Use defaults)

These configurations are optional, and default settings have been defined to help you get started with your cluster. Turn off "Use defaults" to modify these settings now.

Virtual private cloud (VPC)  
This VPC defines the virtual networking environment for this cluster.  
Lab VPC  
vpc-006870684db897fb

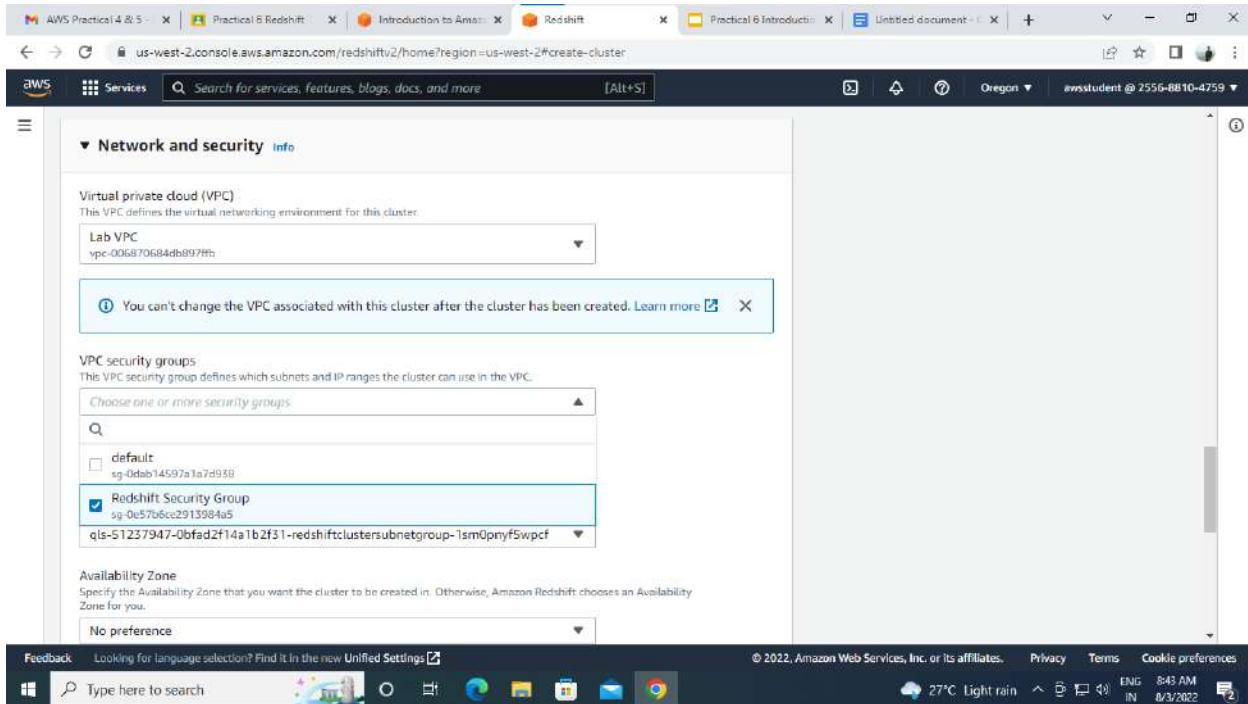
Info You can't change the VPC associated with this cluster after the cluster has been created. Learn more [?](#) X

VPC security groups  
This VPC security group defines which subnets and IP ranges the cluster can use in the VPC.  
Choose one or more security groups  
default  
sg-0daab14597a1a7d938

Feedback Looking for language selection? Find it in the new Unified Settings [?](#)

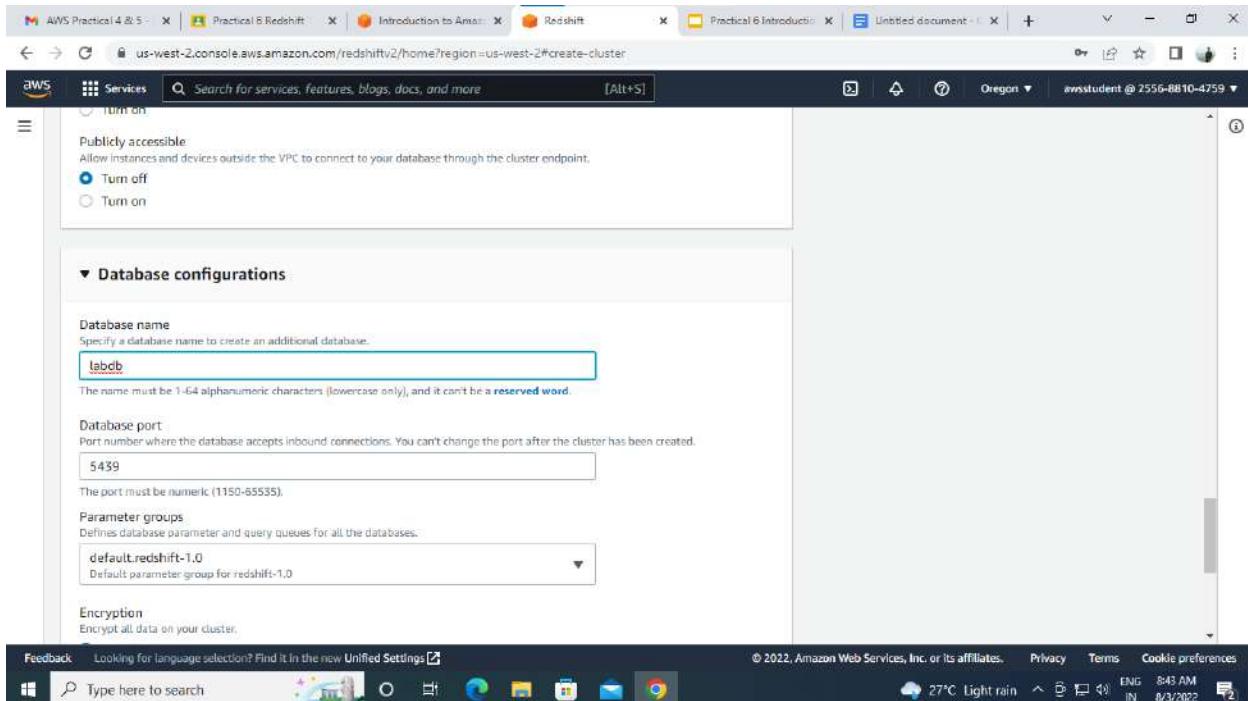
© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Windows taskbar: Type here to search, 27°C Light rain, ENG 8:42 AM IN 8/3/2022

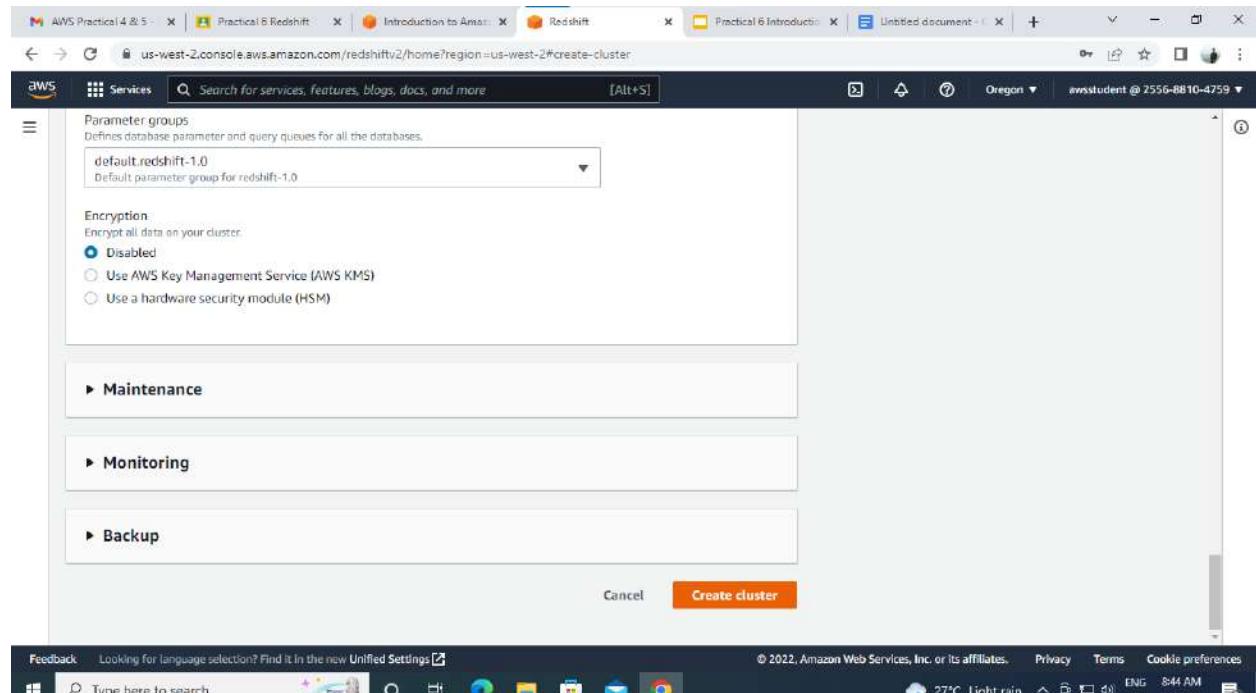


## Step 10 – Expand Database configurations, then configure:

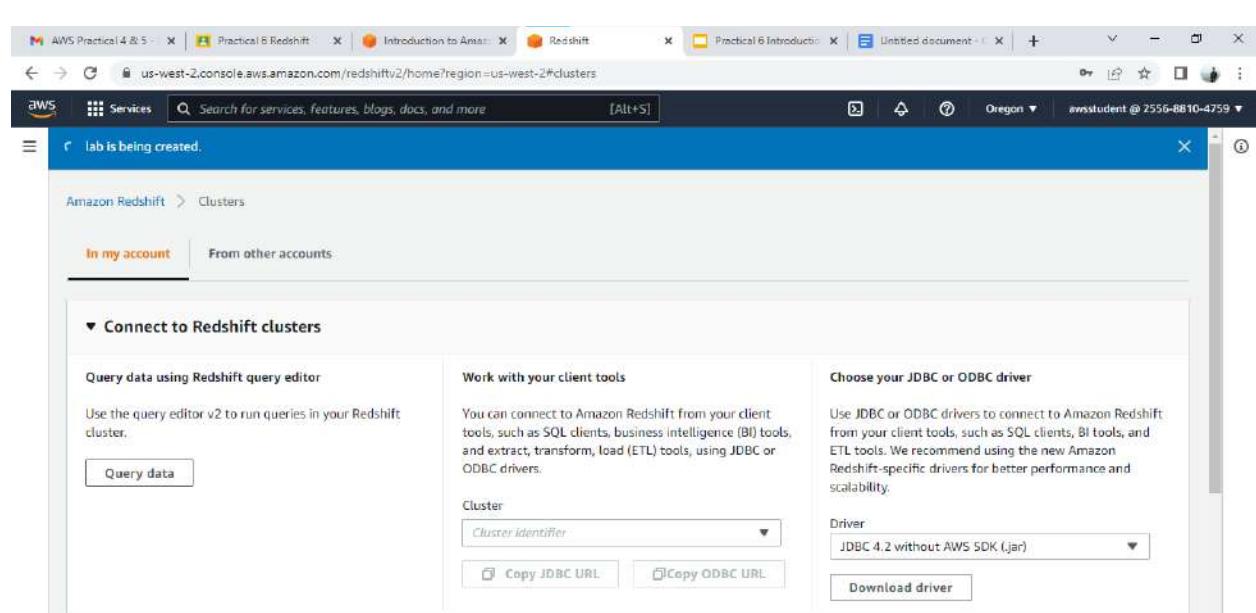
- Database name: labdb



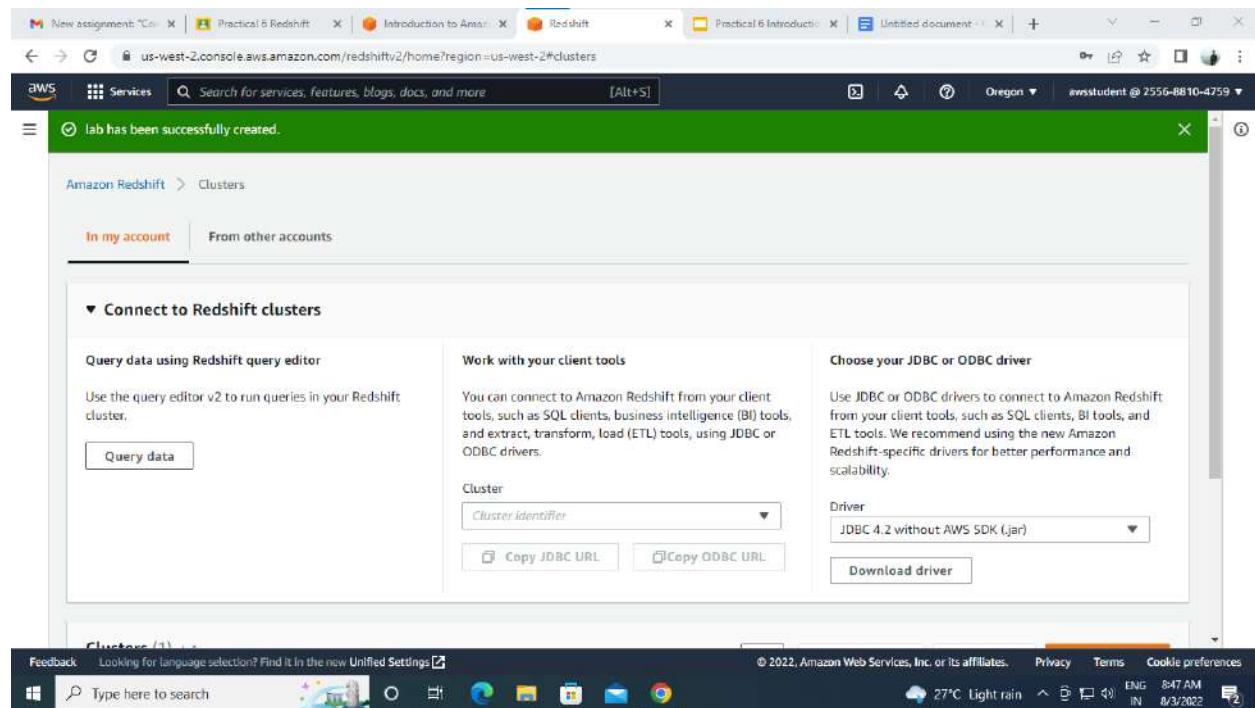
**Step 11 – Scroll to the bottom of the screen, then click **Create cluster** button.**



The screenshot shows the 'Create cluster' wizard on the AWS Redshift console. The current step is 'Parameter groups'. It displays a dropdown menu for selecting a parameter group, with 'default.redshift-1.0' selected. Other options include 'Encryption' (disabled), 'AWS KMS', and 'HSM'. Below the parameter group section are sections for 'Maintenance', 'Monitoring', and 'Backup'. At the bottom right is a large orange 'Create cluster' button.

The screenshot shows the 'Clusters' page on the AWS Redshift console. A blue banner at the top indicates 'lab is being created.' The main area shows a table with one row, labeled 'Clusters (1)'. The table has columns for 'Cluster identifier', 'Status', 'Type', 'Nodes', 'Owner', and 'Actions'. The single cluster listed is 'redshift-1'. At the bottom of the page is a 'Clusters (1)' summary bar.



## 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

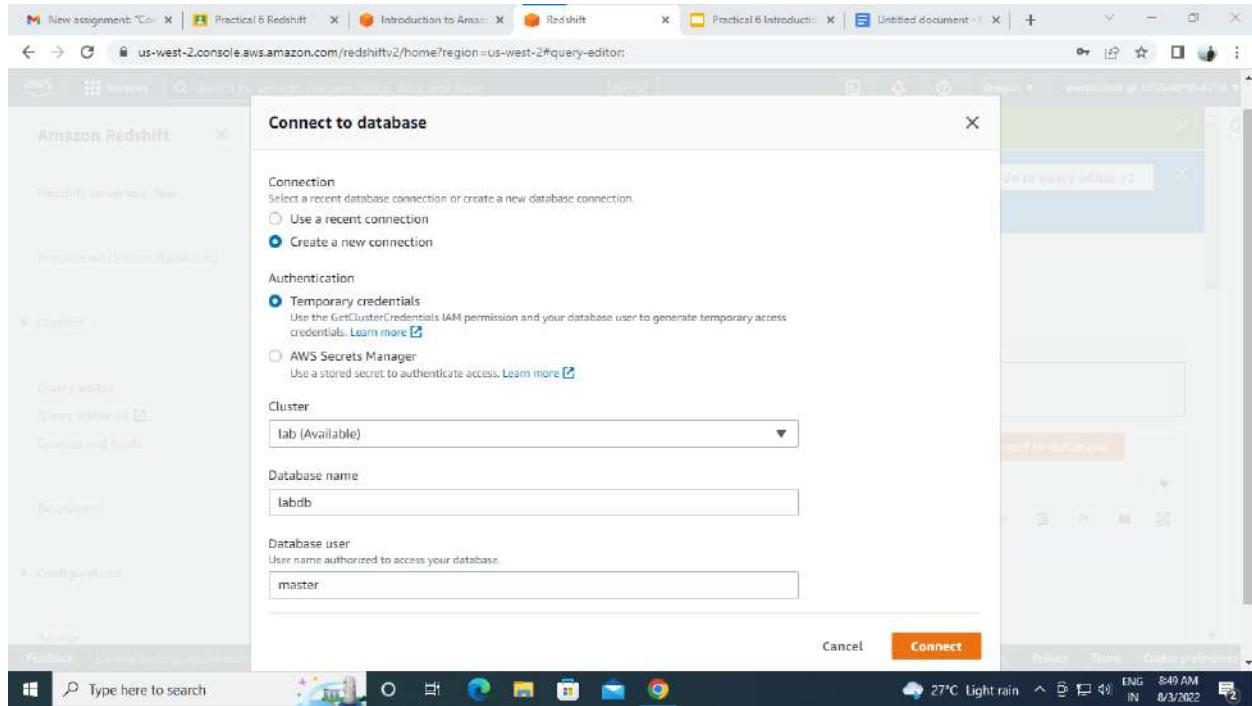
**Step 13 –** In the left navigation pane, choose Explore items.

The screenshot shows the AWS Redshift console with the URL <https://us-west-2.console.aws.amazon.com/redshiftv2/home?region=us-west-2#clusters>. A green banner at the top says "lab has been successfully created." Below it, the "Clusters" section is visible. Under "Connect to Redshift clusters", there are three main sections: "Query data using Redshift query editor", "Work with your client tools", and "Choose your JDBC or ODBC driver". The "Work with your client tools" section includes a dropdown for "Cluster Identifier" (set to "Cluster"), a "Copy JDBC URL" button, and a "Copy ODBC URL" button.

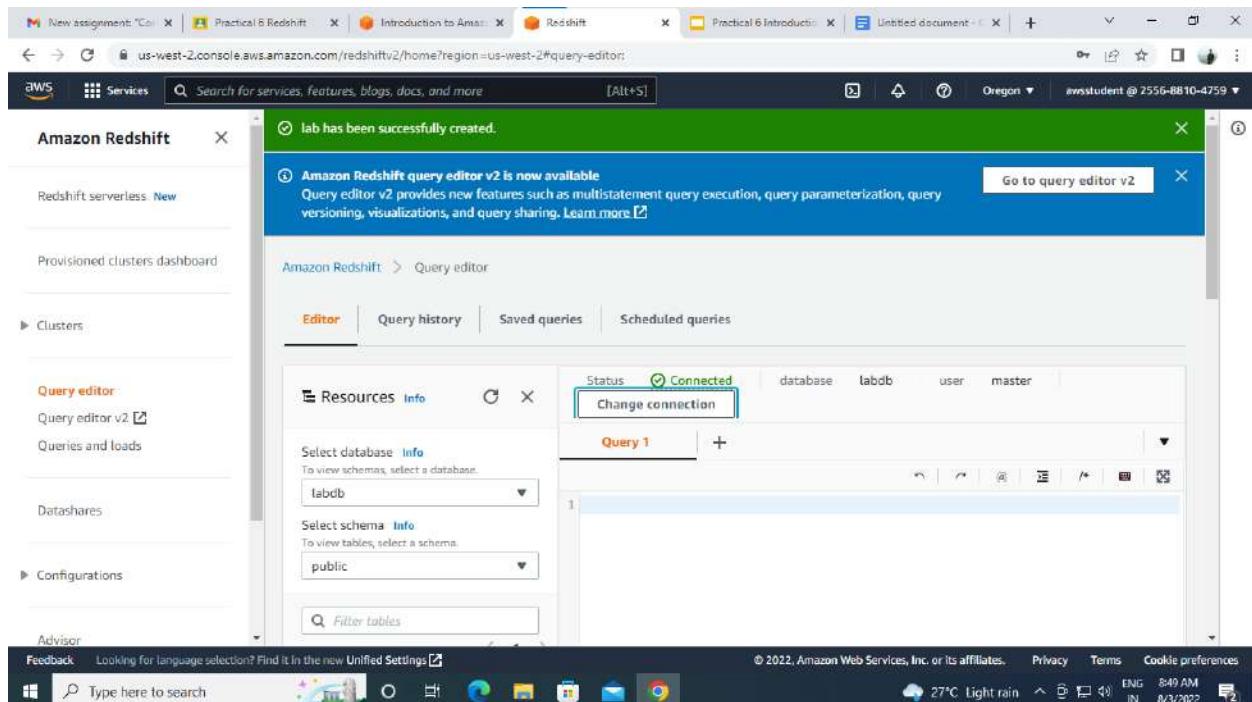
The screenshot shows the AWS Redshift console with the URL <https://us-west-2.console.aws.amazon.com/redshiftv2/home?region=us-west-2#query-editor>. A blue banner at the top says "Amazon Redshift query editor v2 is now available". Below it, the "Query editor" section is visible. It shows a "Resources" panel with dropdowns for "Select database" and "Select schema", and a main area with tabs for "Editor", "Query history", "Saved queries", and "Scheduled queries". A "Connect to database" button is prominently displayed at the top right of the main area.

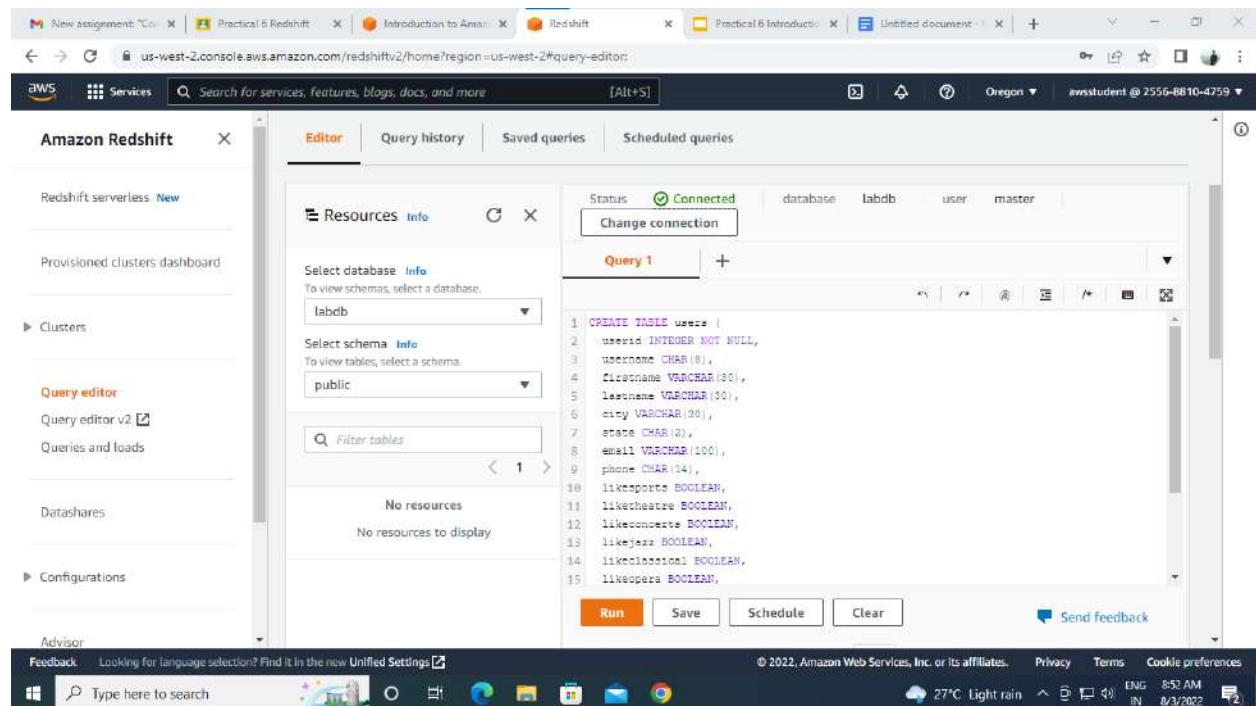
**Step 14 – Click Connect button.**



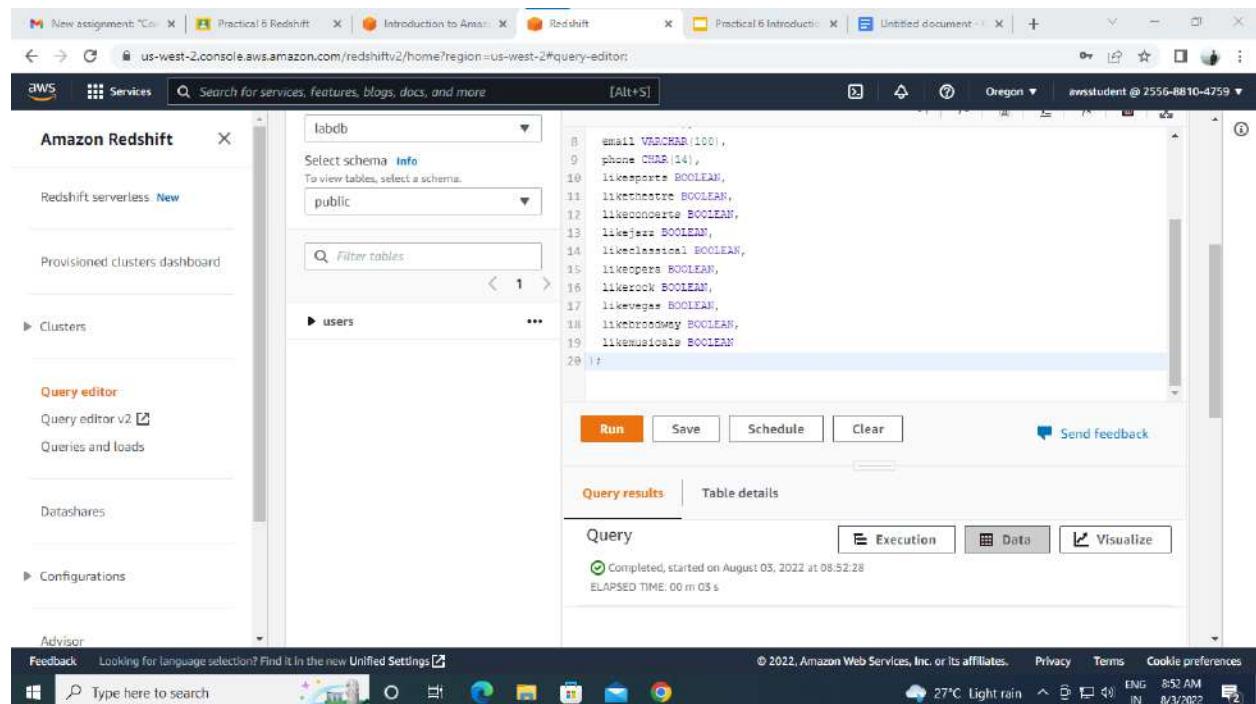
## Task 3: Create a Table

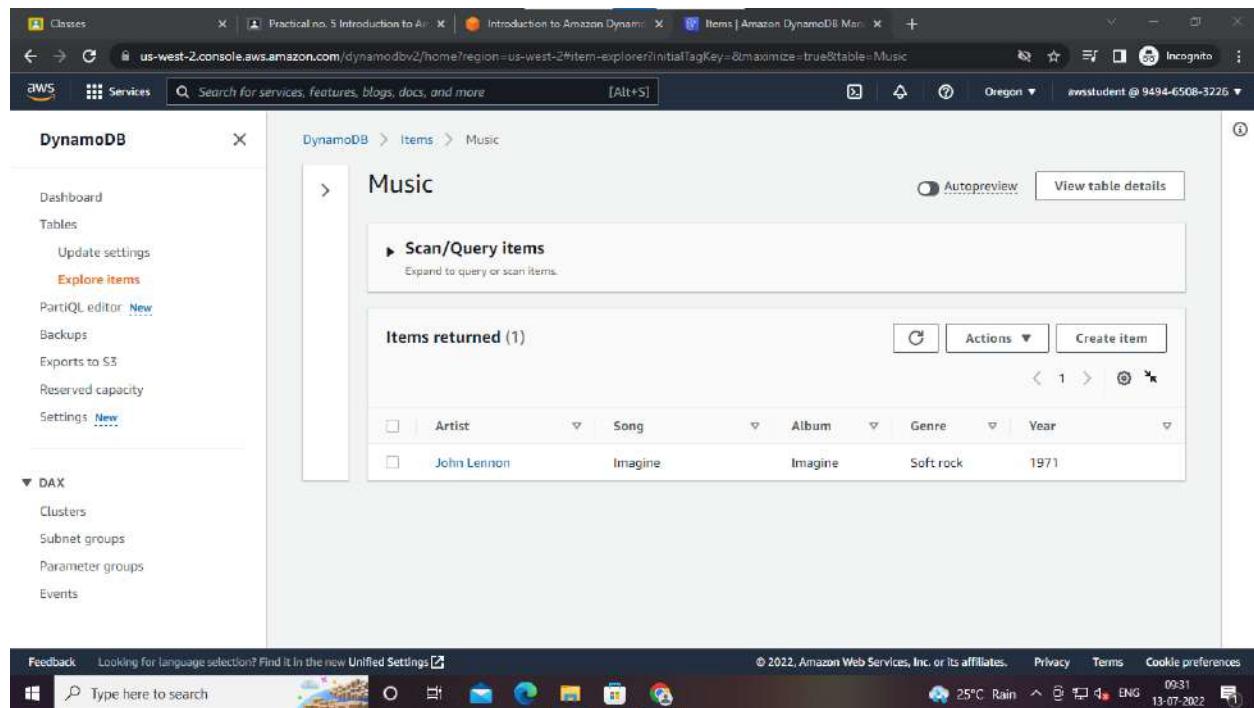
Step 15 – Copy this SQL command and paste it into the Query 1 window, then click





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/ticket/allusers_pipe.txt' CREDENTIALS
```

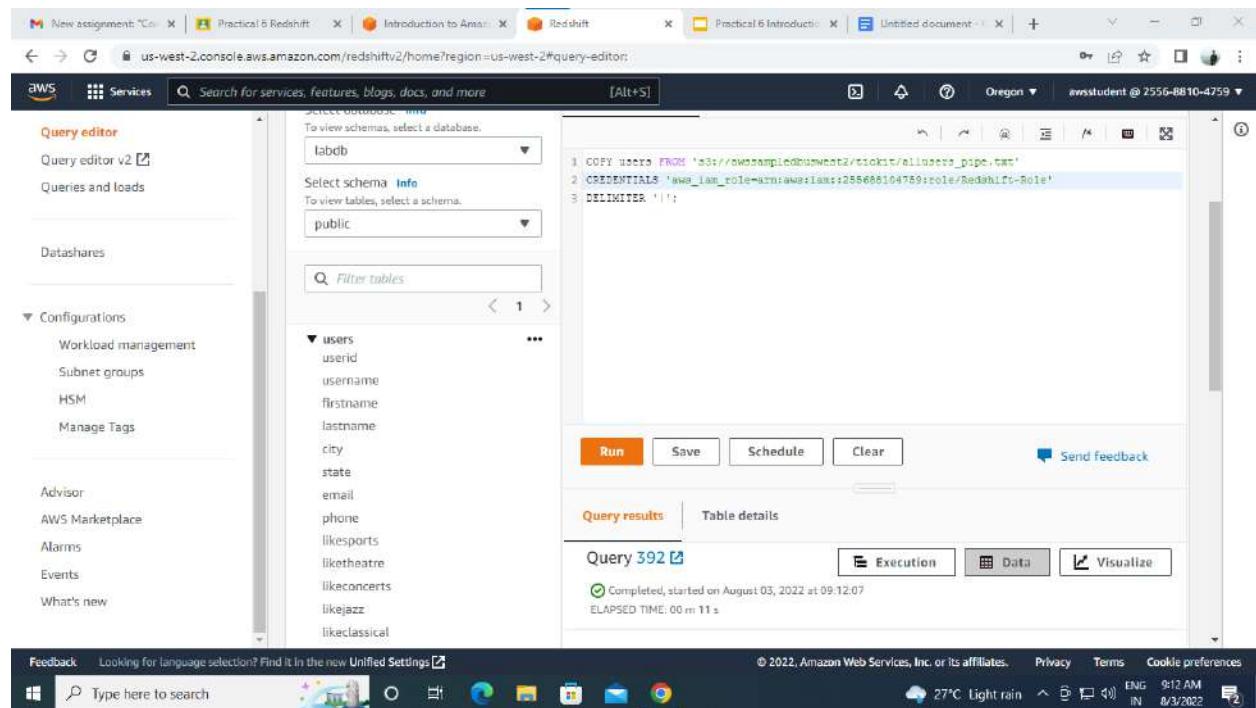
```
'aws_iam_role=YOUR-ROLE' DELIMITER '|';
```

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 screenshot shows the AWS Redshift Query Editor interface. On the left, there's a sidebar with various service links like New assignment, Practical 6 Redshift, Introduction to Amazon Redshift, and Redshift. The main area has tabs for Editor, Query history, Saved queries, and Scheduled queries. A status bar at the top indicates 'Connected' to 'labdb' with 'user' 'master'. Below this, there are dropdowns for 'Select database' (set to 'labdb') and 'Select schema' (set to 'public'). A 'Resources' section shows a tree view with 'users' expanded, listing columns: userid, username, firstname, lastname, city, state, email, phone, likesports, liketheatre, likeconcerts, likejazz, likeclassical, likeopera, likerock, likevegas, likebroadway, and likemusicals. A 'Query 1' tab is active, containing the SQL query: 'SELECT COUNT(\*) FROM users'. The status bar at the bottom right shows the date as 8/3/2022.

This screenshot shows the results of the query from the previous image. The 'Run' button is highlighted in orange. The results table shows a single row with the column 'count' having the value '49990'. The rest of the interface is identical to the first screenshot, including the sidebar, status bar, and bottom navigation.

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;
```

The screenshot shows the AWS Management Console with the Redshift service selected. The left sidebar contains navigation links like 'Query editor', 'Configurations', and 'Advisors'. The main area has tabs for 'Editor', 'Query history', 'Saved queries', and 'Scheduled queries'. A 'Resources' panel on the left lists databases ('labdb') and schemas ('public'). Below it is a table structure for the 'users' table with columns: userid, username, firstname, lastname, city, state. Two queries are open in tabs: 'Query 1' and 'Query 2'. 'Query 1' contains the following SQL:

```

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

Buttons at the bottom of the editor include 'Run', 'Save', 'Schedule', 'Clear', and 'Send feedback'.

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

The screenshot shows the results of the query execution. The 'Table details' section indicates 'Completed' status on August 03, 2022, at 09:14:27, with an elapsed time of 00 m 02 s. The 'Rows returned (18)' section shows the following data:

userid	firstname	lastname	city	state
4343	Abel	Mullins	Commerce	OH
39049	Abraham	Donaldson	Hampton	OH
36418	Amanda	Tran	Concord	OH
24636	Amity	Thomas	Brunswick	OH
39221	Grady	Wilkinson	St. Petersburg	OH
29013	Gregory	Rosario	Saratoga Springs	OH

**Step 22 – Run this query:**

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

The screenshot shows the AWS Management Console with the Redshift service selected. The left sidebar contains navigation links for services like Datasources, Configurations, Advisor, and AWS Marketplace. The main area is the 'Query editor' tab, which is currently active. It displays a list of databases (labdb) and schemas (public). A table named 'users' is shown with columns: userid, username, firstname, lastname, city, and state. Below the table, two tabs are open: 'Query 1' and 'Query 2'. 'Query 2' contains the SQL code provided in the text above. The 'Run' button is visible at the bottom of the editor.

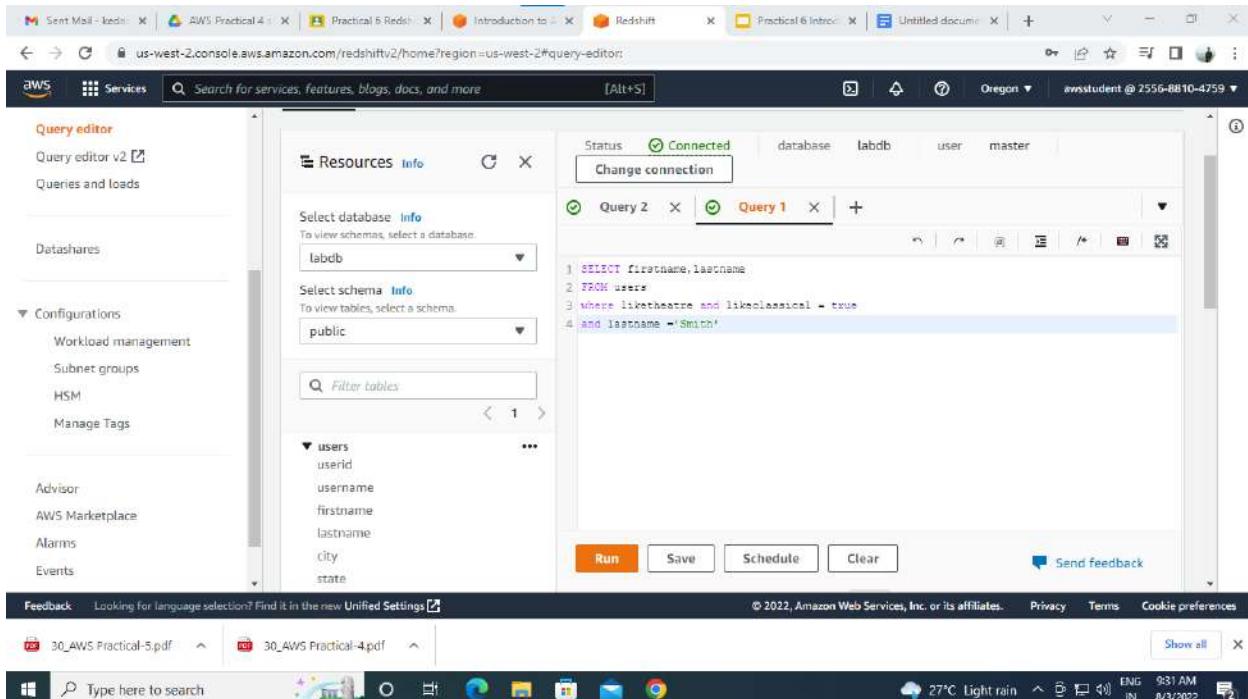
The screenshot shows the results of the query execution. The 'Query results' tab is active, displaying the output of the query. The results table has two columns: 'city' and 'count'. The data is as follows:

city	count
Dover	33
Charleston	30
Hartford	28
Concord	27
Springfield	26
Richmond	24

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



The screenshot shows the AWS Management Console with the Redshift service selected. The left sidebar shows various management options like Datasources, Configurations, and Advisor. The main area is the 'Query editor' where a query is being run:

```

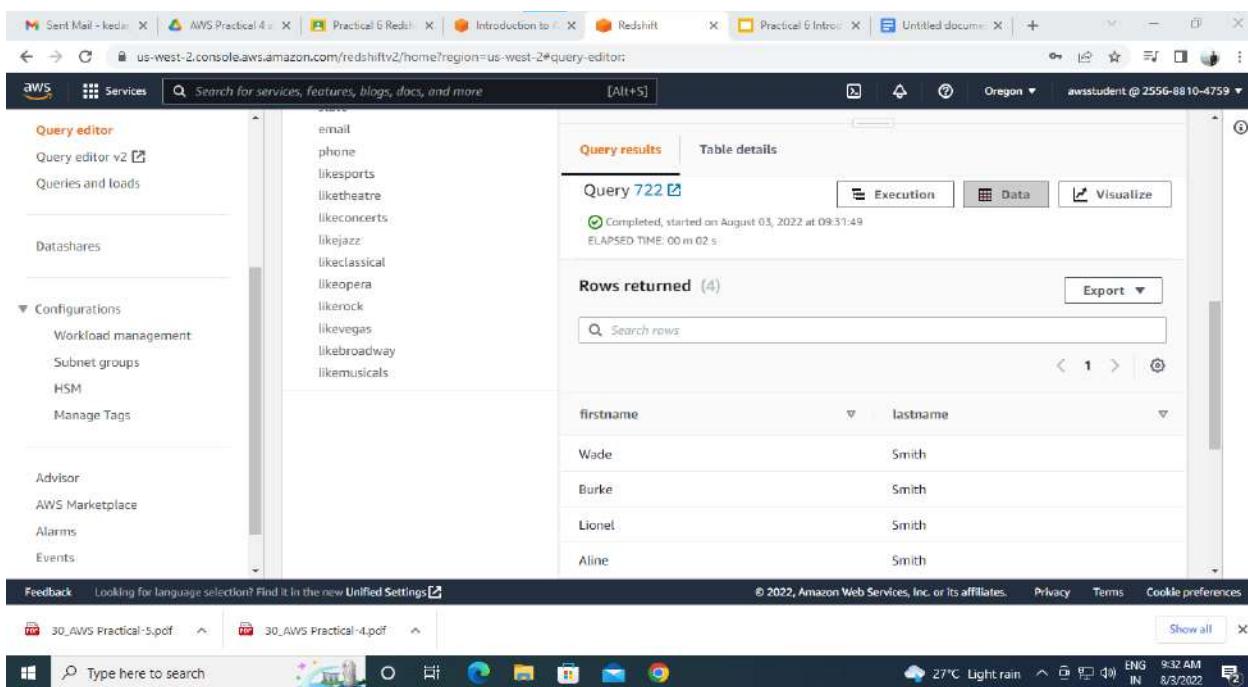
Status Connected database labdb user master
Change connection

Query 2 | Query 1 (highlighted)

1 SELECT firstname, lastname
2 FROM users
3 WHERE liketheatre AND likeclassical = true
4 AND lastname = 'Smith'

```

Below the query, there are buttons for Run, Save, Schedule, Clear, and Send feedback. The status bar at the bottom indicates the query completed successfully.



The screenshot shows the results of the query execution. The left sidebar remains the same. The main area now displays the 'Query results' tab, which shows the following data:

	firstname	lastname
1	Wade	Smith
2	Burke	Smith
3	Lionel	Smith
4	Aline	Smith

At the bottom, there are buttons for Export, Data, and Visualize. The status bar at the bottom indicates the query completed successfully.

## 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](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.**

**Introduction to AWS Device Farm**

Start Lab 00:45:00

# Introduction to AWS Device Farm

45 minutes Free ★★★★ Rate Lab

**aws** training and certification

SPL-27 - Version 1.5.11

© 2022 Amazon Web Services, Inc. or its affiliates. All rights reserved. This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited. All trademarks are the property of their owners.

Note: Do not include any personal, identifying, or confidential information into the lab environment. Information entered may be visible to others.

Overview  
Topics covered  
Prerequisites  
AWS Device Farm Introduction  
AWS Device Farm Terminology  
Start Lab  
Task 1: Locate or Download an Example Android \*.apk or iOS \*.ipa File  
Task 2: Upload and Test the Example Application  
Task 3: Run Test and View the Run's Results  
Conclusion  
End Lab  
Additional Resources

### Step 3 – Download one of the following files.

End Lab 00:44:40

Caution: When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked.  
[Learn more](#)

Open Console

Priority to test in this lab. These examples may move or change from time to time. The test results may vary and may not all pass or fail. Each will provide interesting test results nonetheless.

3. Please download one of the following files to your computer:

- [flickrj-android-sample-android.apk](#)
- [mixarev0.9.2.apk](#)
- [github.com/mehtank/androidminion/releases](#)

4. In the AWS Management Console, on the **Services** menu, click **Device Farm**.

5. If you see **Next**, click it.

6. At the AWS Device Farm window, configure:

- Project Name: `myProject`
- Click **Create**

If you type a project name other than `myProject`, be sure to use it consistently throughout this lab.

Overview  
Topics covered  
Prerequisites  
AWS Device Farm Introduction  
AWS Device Farm Terminology  
Start Lab  
Task 1: Locate or Download an Example Android \*.apk or iOS \*.ipa File  
Task 2: Upload and Test the Example Application  
Task 3: Run Test and View the Run's Results  
Conclusion  
End Lab  
Additional Resources

### Step 4 – Download the file - [flickrj-android-sample-android.apk](#).

File Name	Description	Release Date	Size
flickr-android-1.0.3-20120619135416.jar	Binary Bundle(excluding dependencies) Release 1.0.3-20120619135416	Jun 19, 2012	318.91KB
flickr-android-1.0.2-20120411195700-sources.jar	Source Bundle Release 1.0.2-20120411195700	Apr 11, 2012	172.54KB
flickr-android-1.0.2-20120411195700.jar	Binary Bundle(excluding dependencies) Release 1.0.2-20120411195700	Apr 11, 2012	318.76KB
flickr-android-1.0.1-20111224194607-sources.jar	Source Bundle Release 1.0.1-20111224194607	Dec 24, 2011	172.32KB
flickr-android-1.0.1-20111224194607.jar	Binary Bundle(excluding dependencies) Release 1.0.1-20111224194607	Dec 24, 2011	318.5KB
flickr-android-1.0.0-2011122213155-sources.jar	Source Bundle Release 1.0.0-2011122213155	Nov 25, 2011	172.56KB
flickr-android-1.0.0-2011122213155.jar	Binary Bundle(excluding dependencies) Release 1.0.0-2011122213155	Nov 23, 2011	318.62KB
flickr-android-sample-android.apk	Android Sample App	Oct 24, 2011	144.5KB

## Step 5 – Click on Open Console button.

**End Lab** **00:39:36**

This automatically logs you in to the AWS Management Console.

**Caution:** When you are in the console, do not deviate from the lab instructions. Doing so may cause your account to be blocked. [Learn more](#).

**Open Console**

**Common Login Errors**

**Error: Federated login credentials**

Your unique, federated login credentials are being created. Please try again in 30 seconds.

If you see this message:

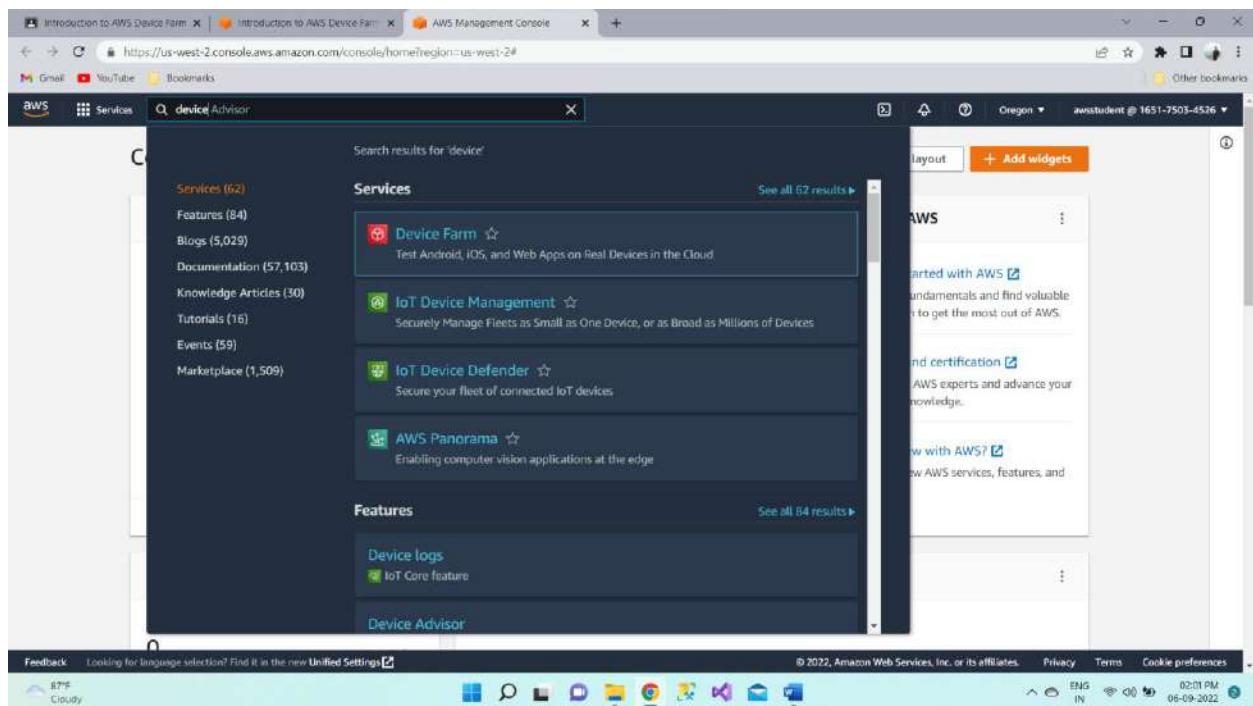
- Close the browser tab to return to your initial lab window
- Wait a few seconds
- Choose **Open Console** again

You should now be able to access the AWS Management Console.

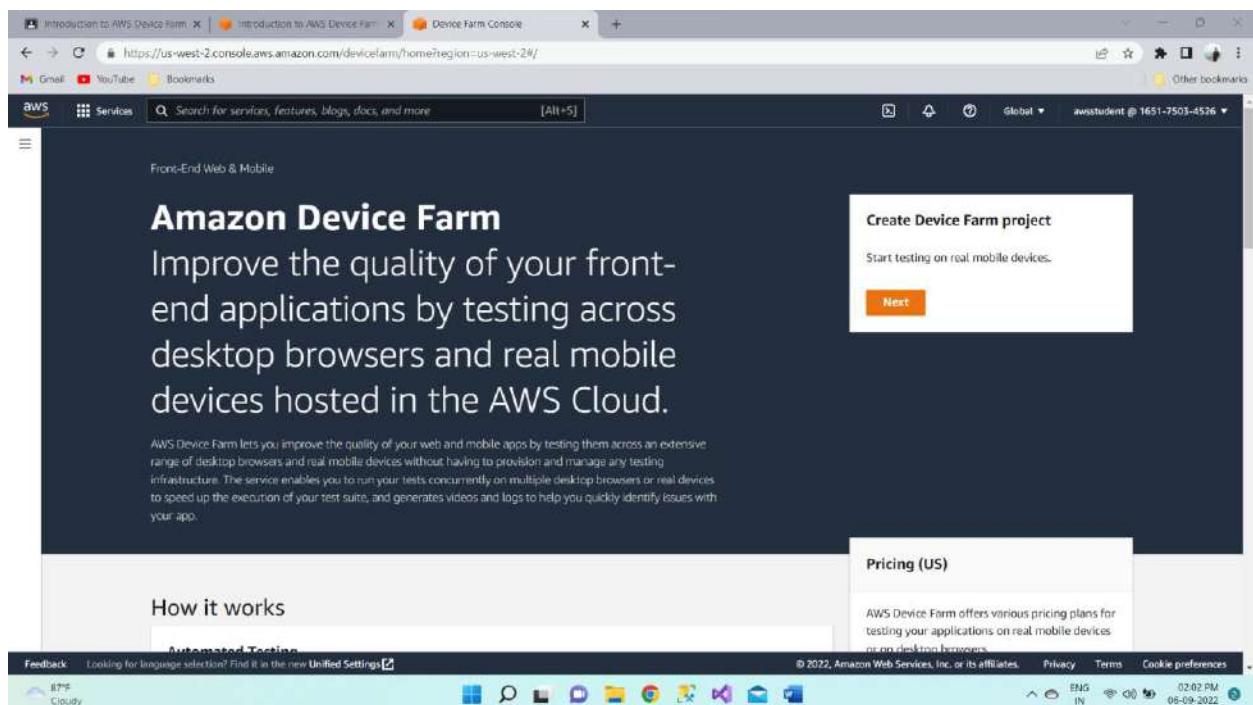
**Error: You must first log out**

**Amazon Web Services Sign In**

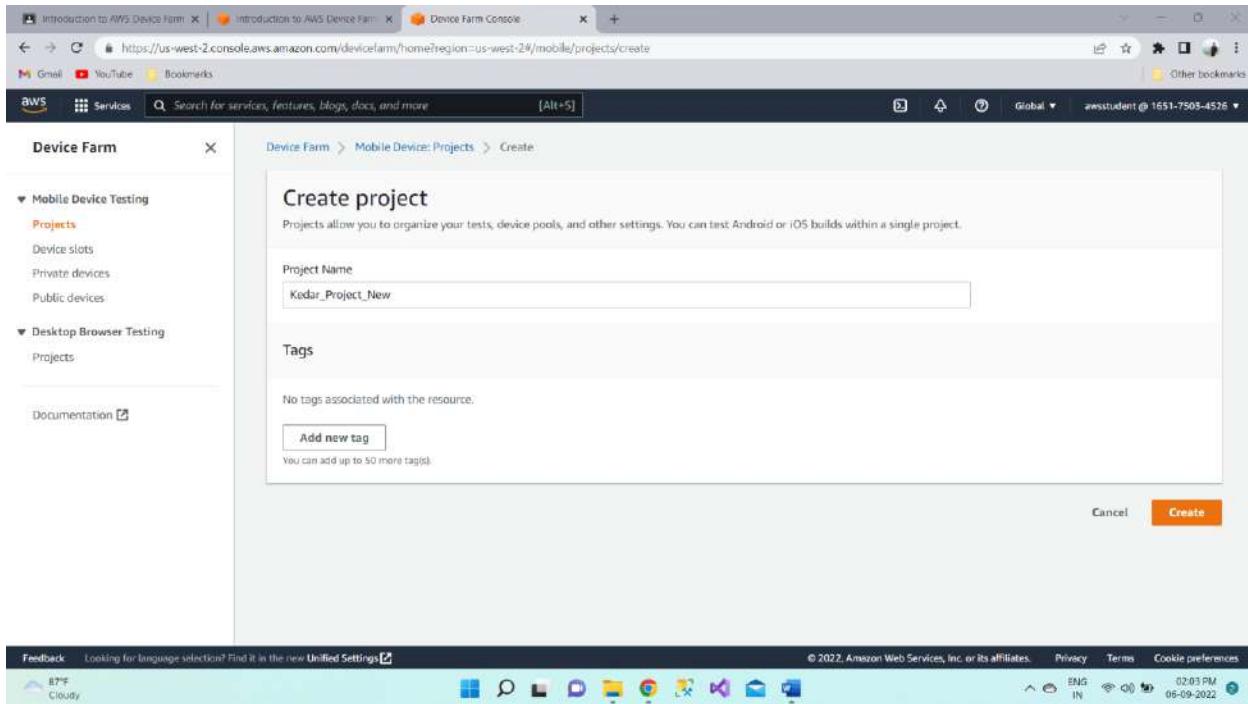
## Step 6 – In the Service search bar, search Device Farm.



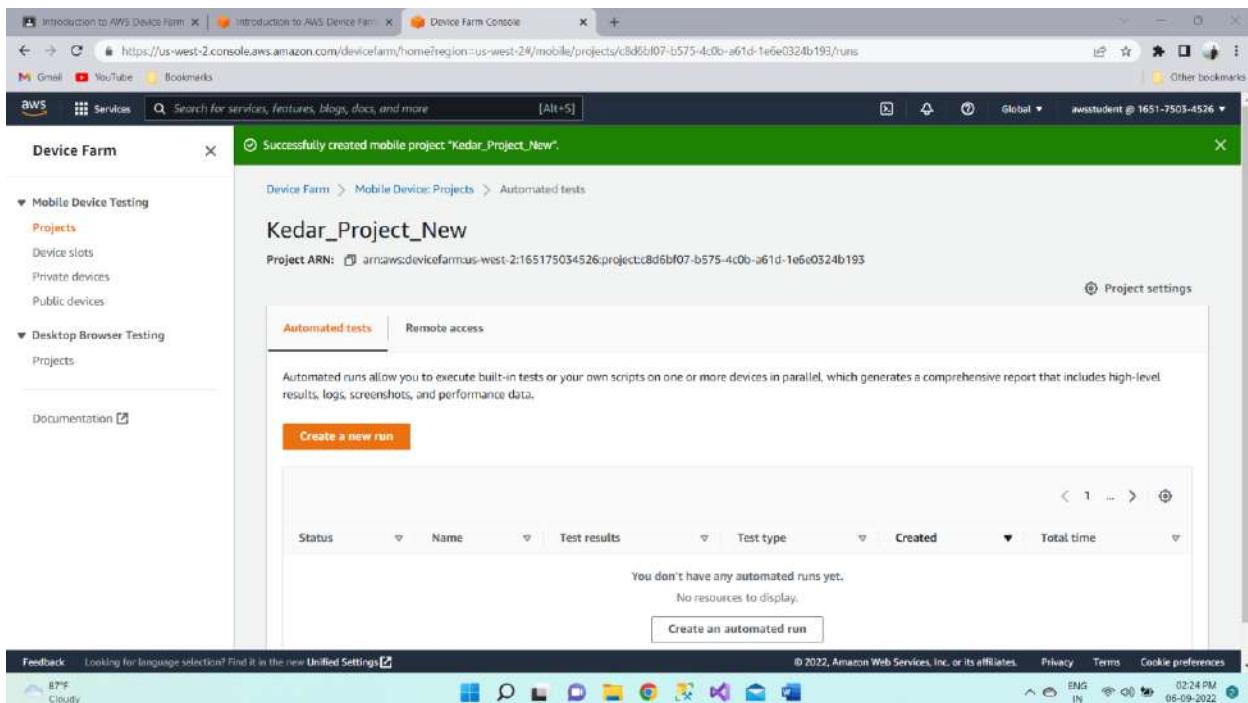
**Step 7 – Click on Next button.**



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

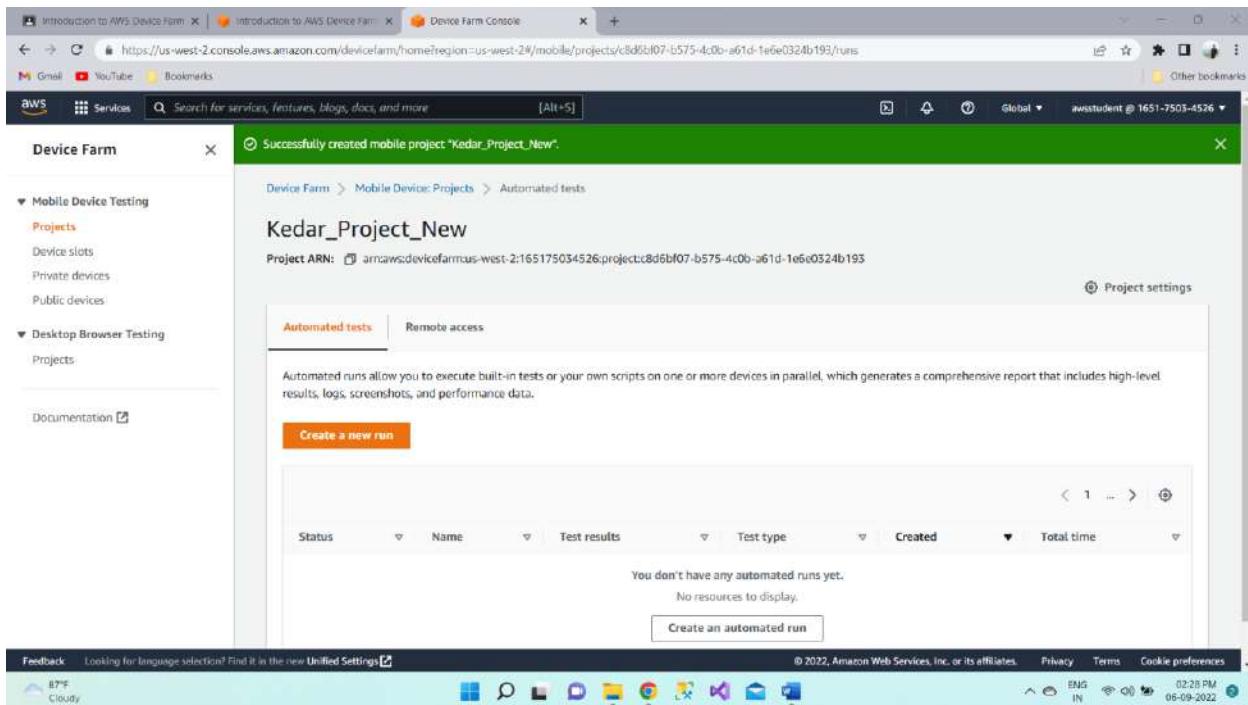


New project is created.



## 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.

Device Farm > Mobile Device Projects > Automated tests > Create

Step 1 Choose application

Step 2 Configure

Step 3 Select devices

Step 4 Specify device state

Step 5 Review and start run

**Choose application**

Mobile App Web App

Upload an Android app as a .apk. Upload an iOS app as a .ipa. Be sure to build for 'iOS device'. No instrumentation or provisioning required.

Choose File or drop file here

Cancel Next

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Cloudy ENG IN 02:31 PM 06-09-2022

Open This PC > Downloads >

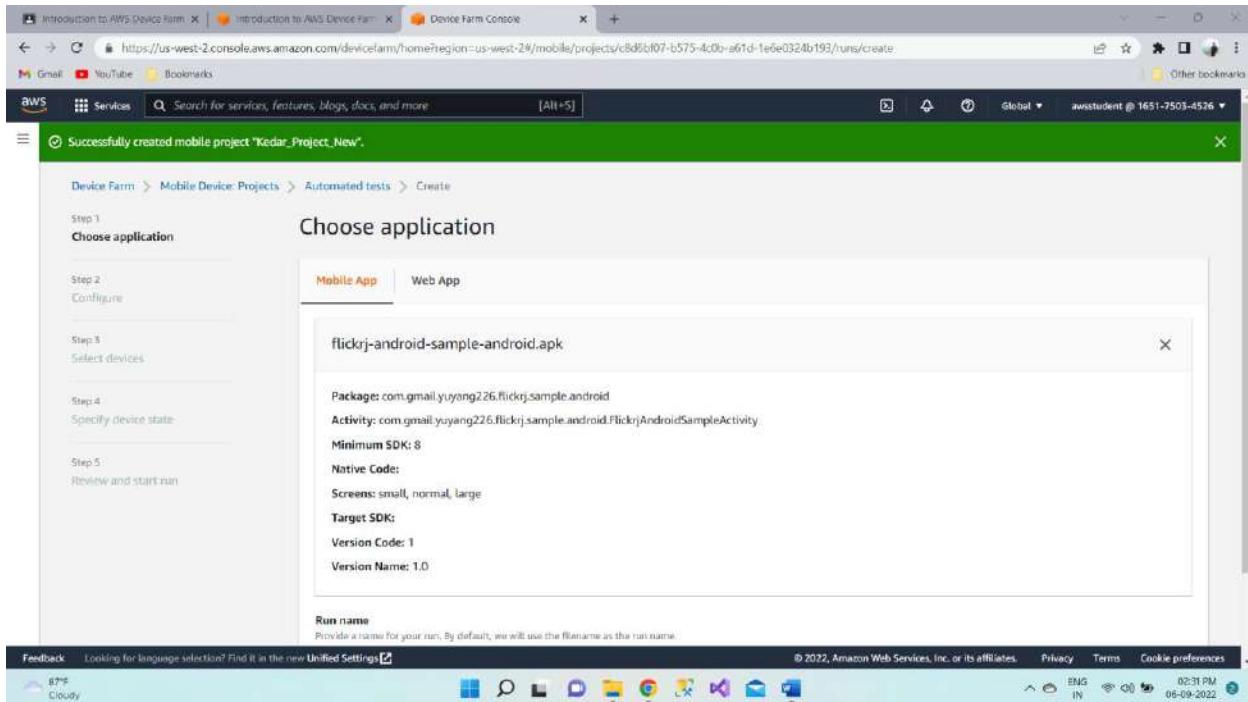
Name Date modified Type Size

flickr-android-sample-android.apk	06-09-2022 01:59 PM	APK File	145 KB
24_AWS_Practical_7	06-09-2022 01:41 PM	Microsoft Word Document	3,659 KB
VMware-Horizon-Client-2206-B.6.0-2009430	01-09-2022 01:19 PM	Application	4,17,125 KB
621_KedarJadhav_AWS-IA 2 Assignment	30-08-2022 11:07 PM	Microsoft Edge PDF	1,527 KB
607_Vikas_Mishra	30-08-2022 09:44 PM	Microsoft Edge PDF	3,720 KB
onlinecoursesaptelac.in_hoc22_cse3_unit_unit=17&assessment=95	30-08-2022 08:53 PM	IMG File	634 KB
UlfathSudhakarCommunity (1)	29-08-2022 05:59 PM	Windows Installer	11,41,028 KB
24_NLPPractical_1	29-08-2022 06:39 AM	Jupyter Source File	2,317 KB
24_NLP_Practical_3	29-08-2022 06:39 AM	Jupyter Source File	21 KB
24_NLPPractical_1_Inaugural	29-08-2022 06:39 AM	Jupyter Source File	45 KB
24_NLPPractical_1_UsersJoint	29-08-2022 06:38 AM	Jupyter Source File	48 KB
CFG	29-08-2022 06:36 AM	Jupyter Source File	22 KB
DLNLP_Speech_And_Text	29-08-2022 06:34 AM	Jupyter Source File	8 KB
Read, Write, and Append Data in Excel - Example	29-08-2022 06:15 PM	File Folder	
Last month (30)			
24_Practical_2	28-08-2022 10:29 PM	Microsoft Edge PDF	281 KB
quickstart-master	27-08-2022 06:26 PM	Compressed (zipped)	22 KB

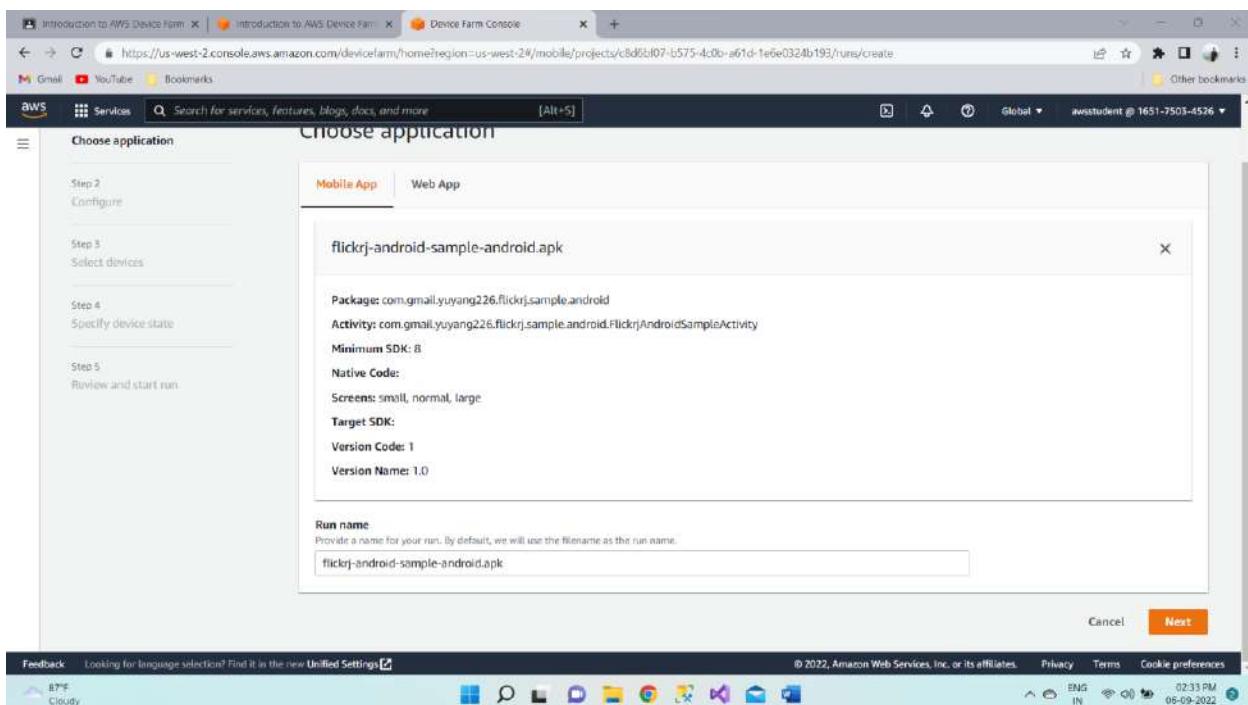
File name: flickr-android-sample-android.apk

All Files Open Cancel

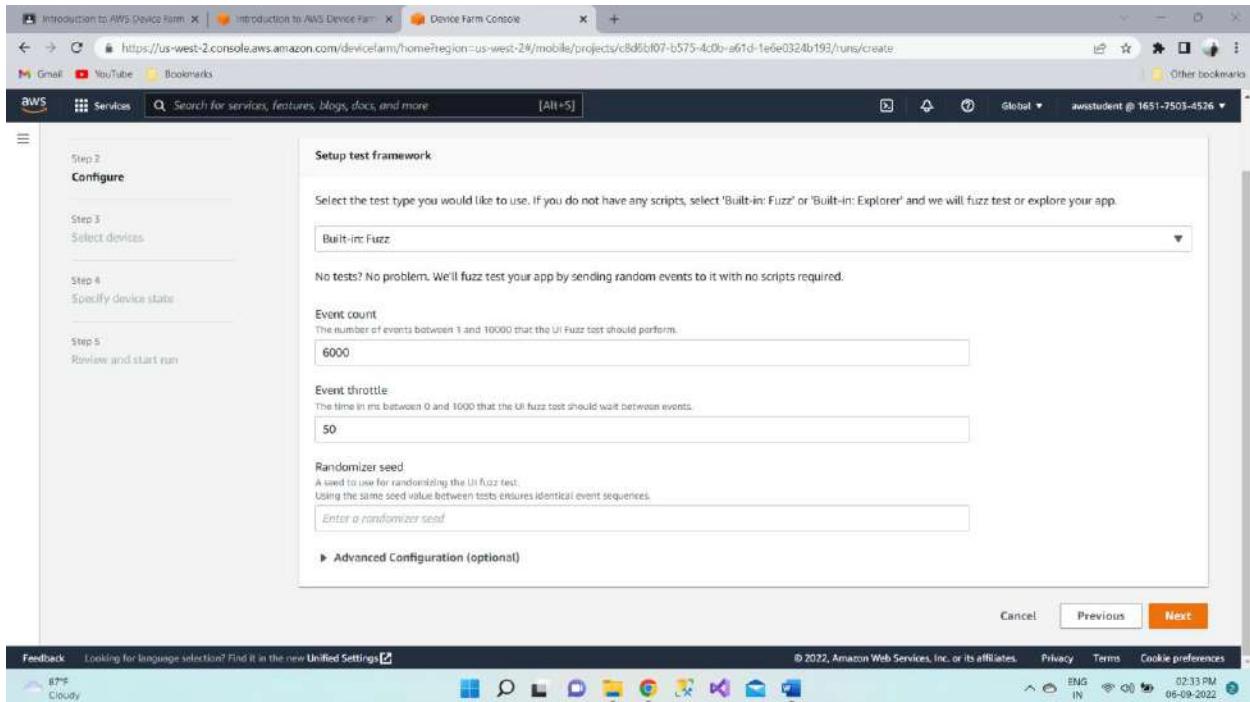
Cloudy ENG IN 02:31 PM 06-09-2022



## Step 11 – Click Next.

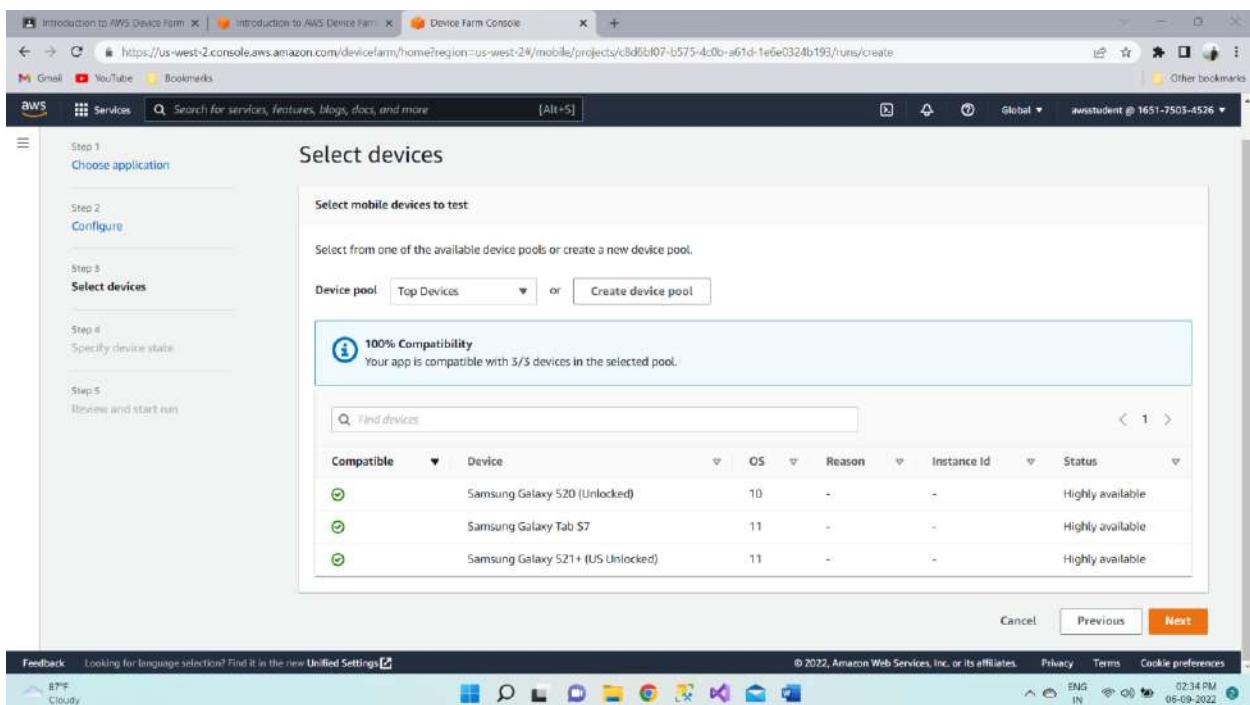


## Step 12 – Click Next.

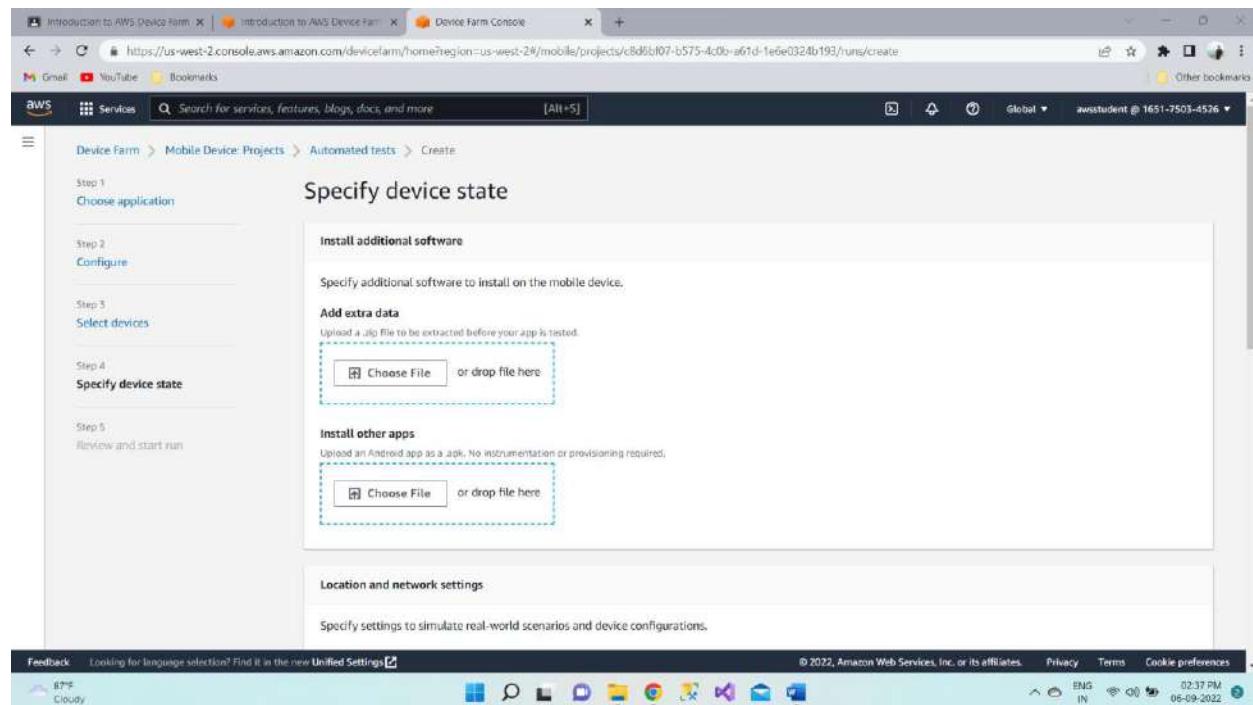


### Step 13 – On the Select devices page, Click Next.

You will see the Top Devices pool.



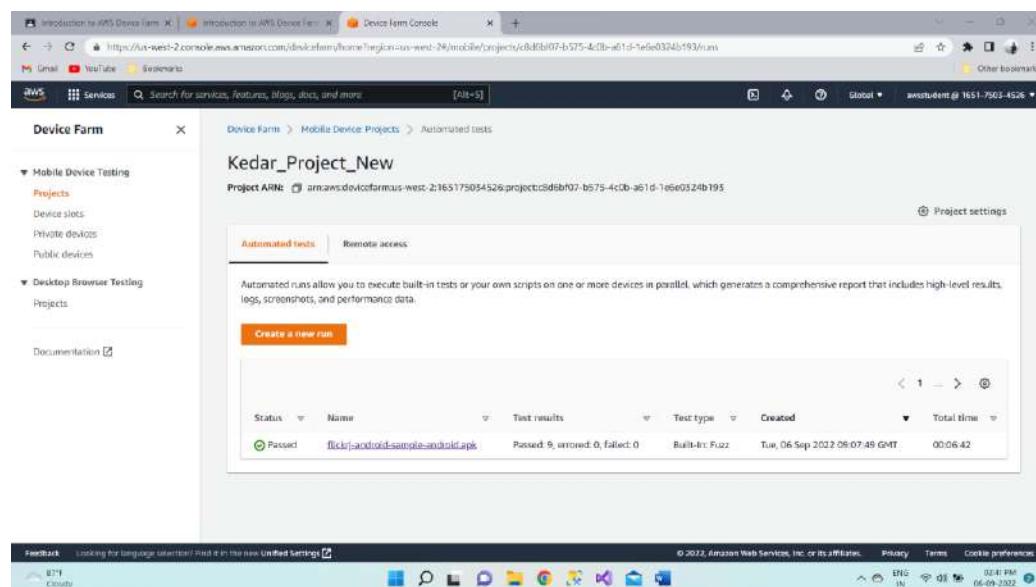
### Step 14 – On the Specify device state page, Click Next.



### 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



## 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’s 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

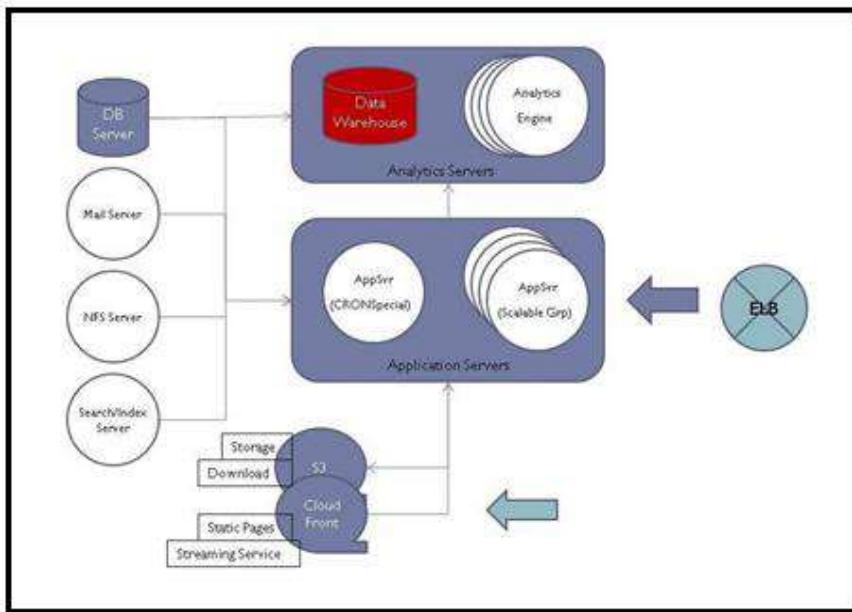
- Amazon Web Services (AWS) has been the foundation of Classle's infrastructure since the company's inception. Vaidya Nathan, Founder and CEO-Classle, explains that AWS allowed the company to begin operations six months ahead of schedule and more economically than had been anticipated. Classle is also 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.

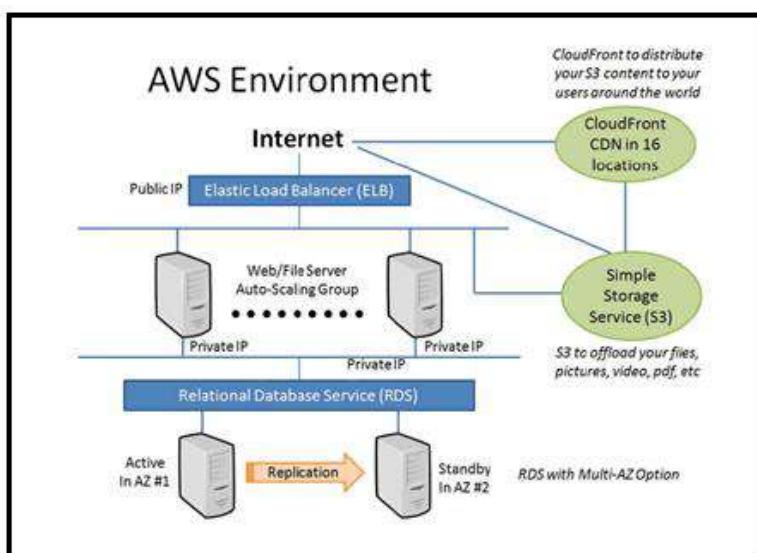
### 2. Before Cloud

- 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

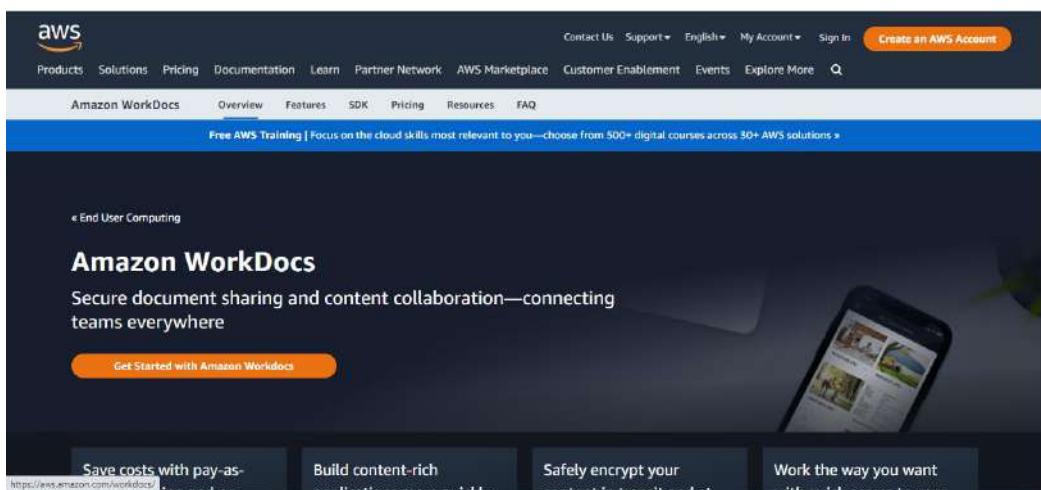
- 2) Amazon S3
- 3) Amazon CloudFront
- 4) Elastic Load Balancing
- 5) Amazon RDS

## 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:

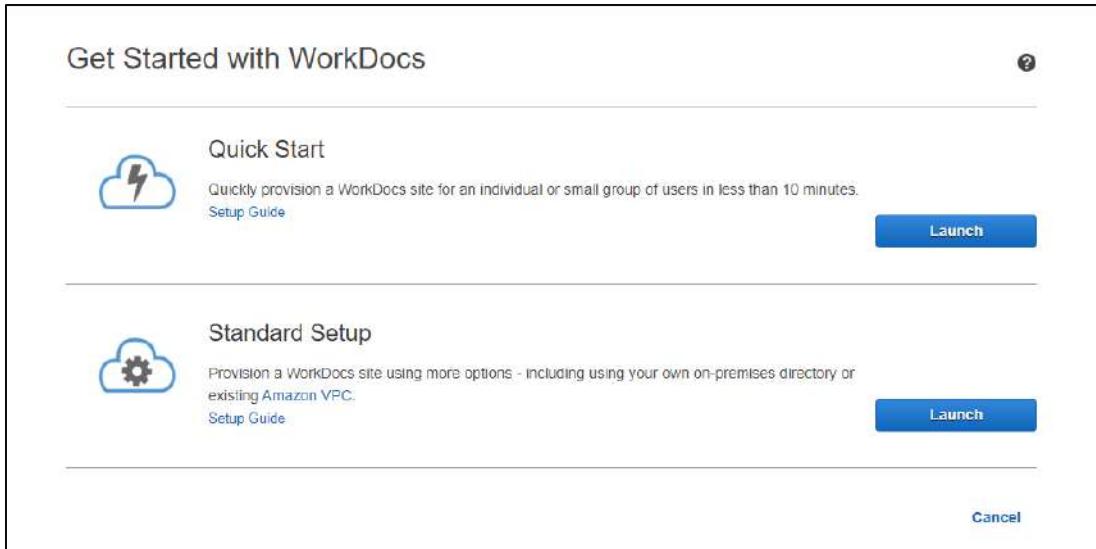
**Step 1:** Go to the particular link - <https://aws.amazon.com/workdocs/>



**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.



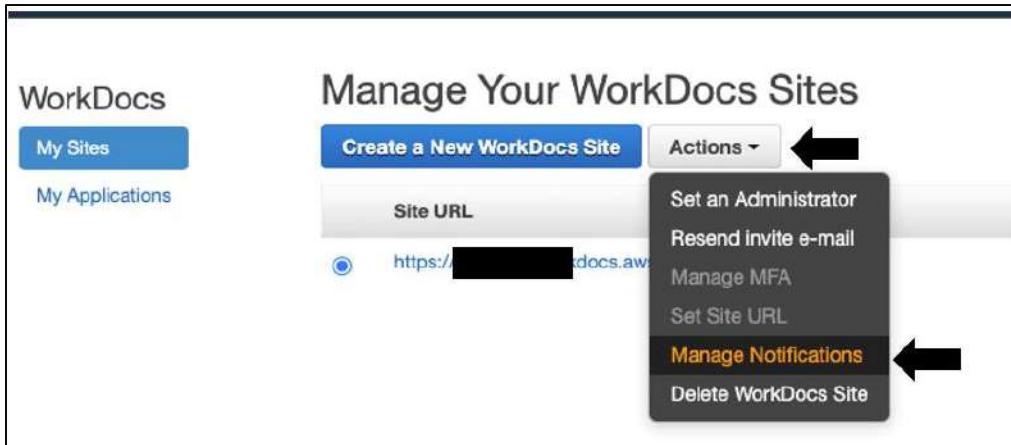
**Step 5:** On the next page, you need to specify the site URL, email and name details as shown in the following figure.

The screenshot shows the 'WorkDocs Quick Start' configuration form. It includes a sidebar with 'WorkDocs', 'My Sites', and 'My Applications'. The main area has a title 'WorkDocs Quick Start' and a description of the setup process. It contains fields for 'Region' (set to Asia Pacific (Singapore)), 'Site URL' (set to https://vembudocs.awsapps.com/workdocs), and 'Set WorkDocs Administrator' fields for 'Email', 'First Name', and 'Last Name', all of which are redacted with black bars. At the bottom are 'Cancel' and 'Complete Setup' buttons.

**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.

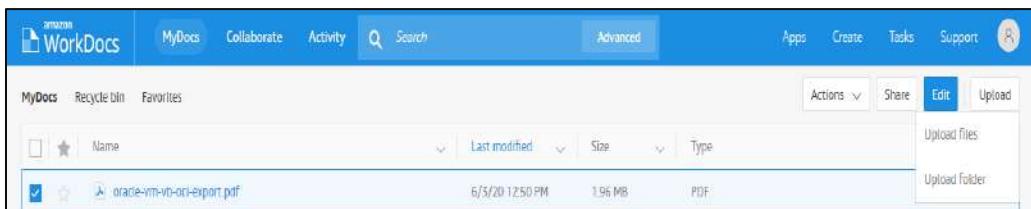
**Step 8:** If you didn't get an invite mail yet, select your created WorkDocs site, click Actions, and select Resend invite e-mail as shown in the following figure.



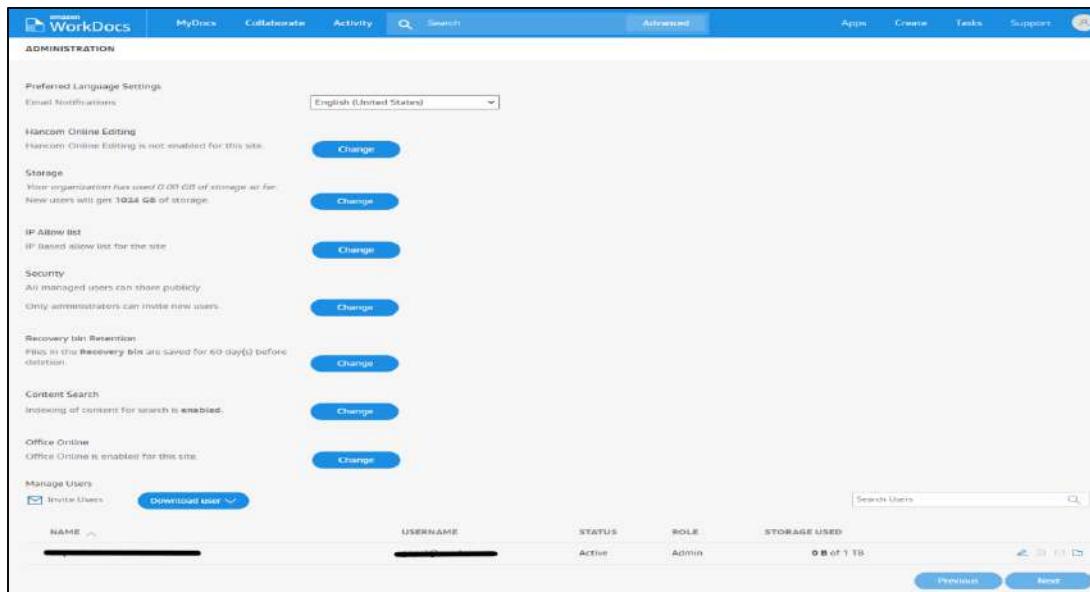
**Step 9:** Now, click your WorkDocs site link, type your registered email ID and login to WorkDocs console. You will see the WorkDocs console similar to as shown in the following figure.



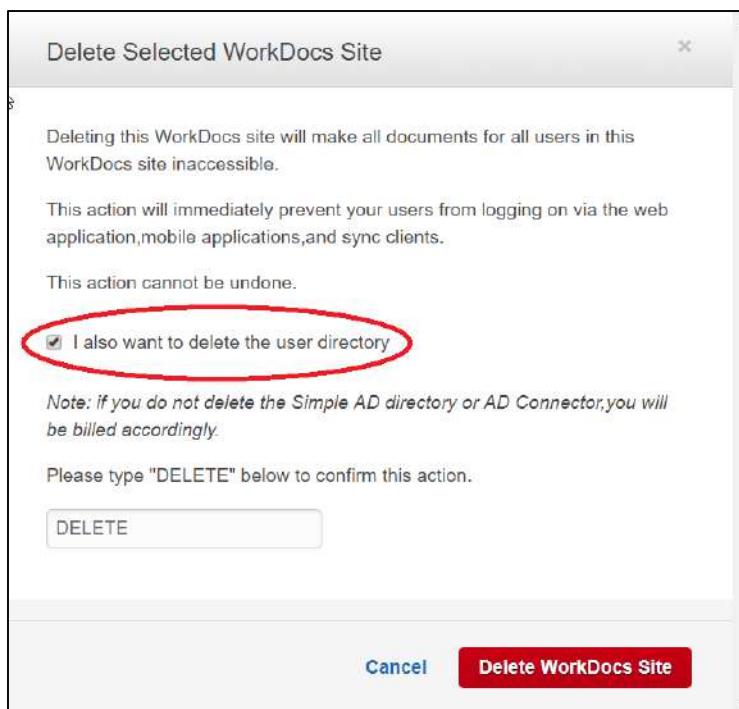
**Step 10:** In the right pane, you have various options to upload files and folders or create a new folder structure as shown in the following figure.



**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.

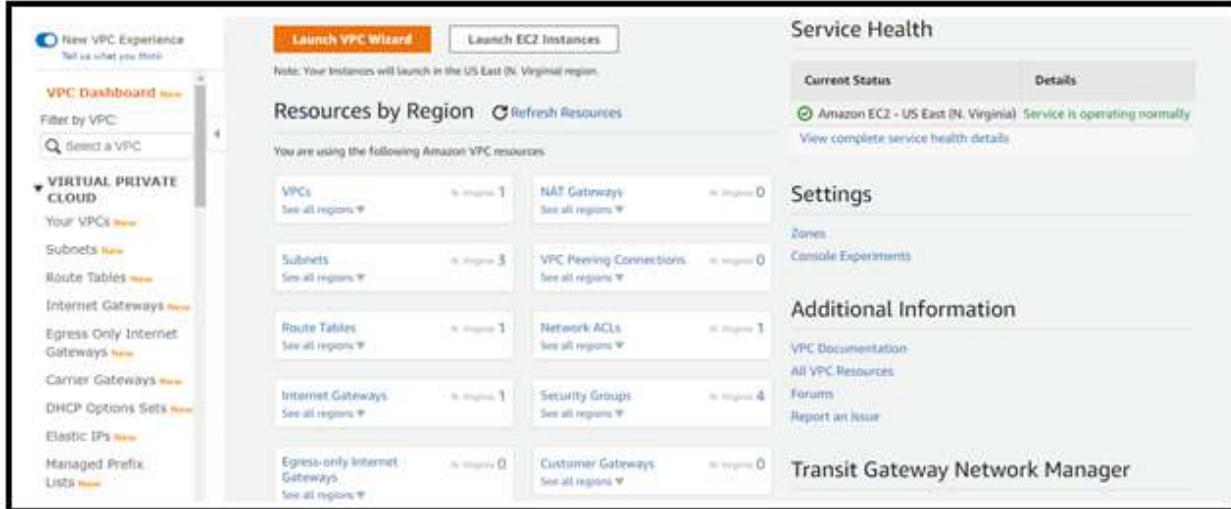
Recommended links:

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

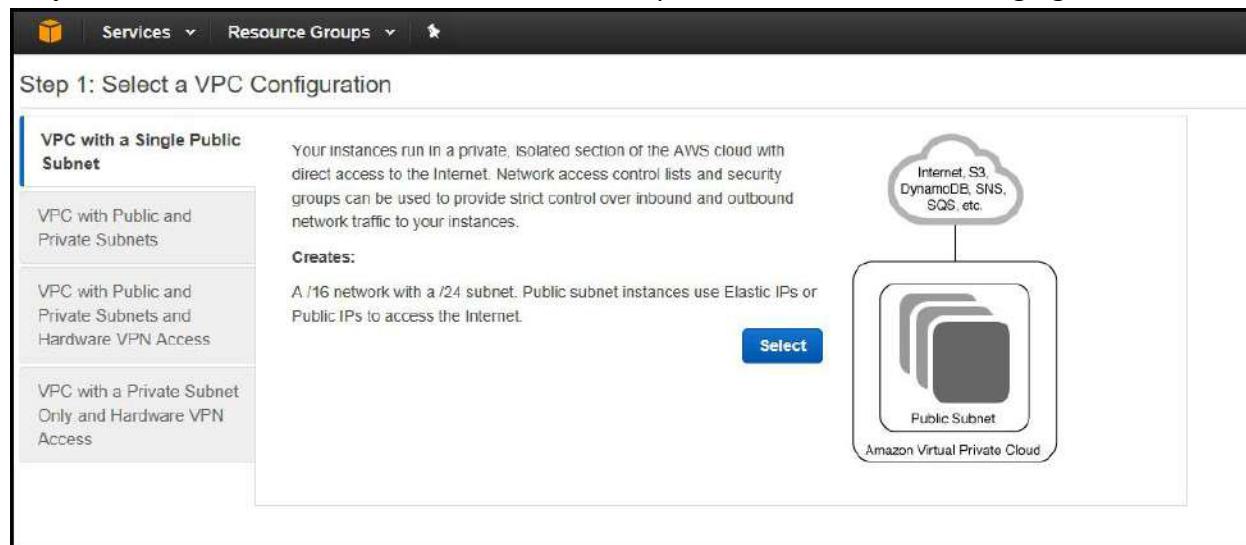
## 1. Creating VPC in AWS Cloud

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 VPC 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 2: VPC with a Single Public Subnet

IPv4 CIDR block: 10.0.0.0/16 (65531 IP addresses available)
IPv6 CIDR block: <input checked="" type="radio"/> No IPv6 CIDR Block <input type="radio"/> Amazon provided IPv6 CIDR block
VPC name:
Public subnet's IPv4 CIDR: 10.0.0.0/24 (251 IP addresses available)
Availability Zone: No Preference
Subnet name: Public subnet
You can add more subnets after AWS creates the VPC.
Service endpoints
Add Endpoint
Enable DNS hostnames: <input checked="" type="radio"/> Yes <input type="radio"/> No
Hardware tenancy: Default

**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](Http://docs.aws.amazon.com/amazonVPC/latest/UserGuide/VPC_Subnets.html)

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

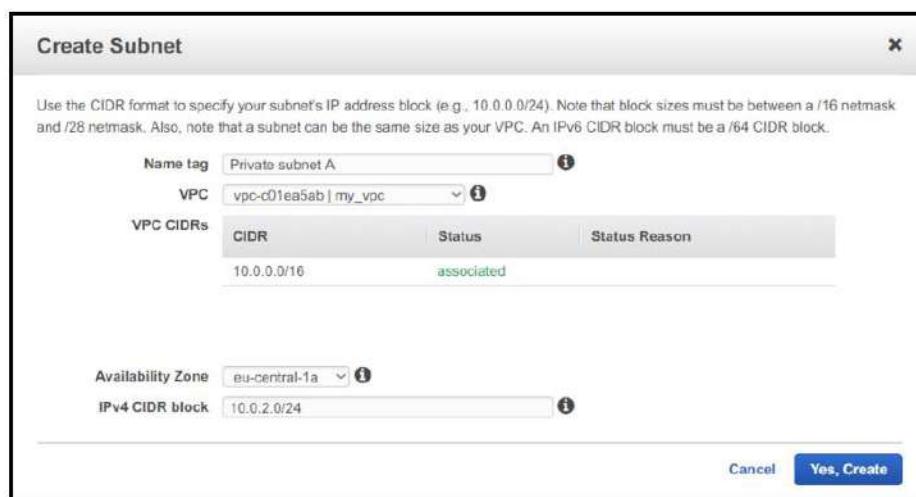
**Step 1:** Select the Subnets option in the navigation pane and then click Create Subnet.

**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
- **Ipv4 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.

