



Hindi Vidya Prachar Samiti's
Ramniranjan Jhunjhunwala College of Arts,
Science & Commerce (Autonomous),
Ghatkopar(W) MUMBAI - 400 086

DEPARTMENT OF INFORMATION TECHNOLOGY
2022 - 2023

M.Sc. (I.T.) SEM III
Cloud Solution Architect - AWS

Name: Pavan Ashok Yadav

Roll No.: 620

INDEX

Practical No.	Title	Date	Page No
1	Introduction: Getting Familiarized with AWS Console. <ul style="list-style-type: none"> A. Creating Aws Free Tier Account B. Getting Familiarized with The Aws Console 	15/06/2022	1-11
2	An Aws Iam User: Creating an AWS IAM User. <ul style="list-style-type: none"> A. Explore users and groups. B. Add users to groups C. Sign-In and test the users 	24/06/2022	12-42
3	Working With S3 Buckets <ul style="list-style-type: none"> A. Create a bucket. B. Upload an object to the bucket. C. Make an object public D. Create a bucket policy E. Explore versioning 	29/06/2022	43-63
4	Introduction to AWS Key management Service <ul style="list-style-type: none"> 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 	05/07/2022	64-90
5	Introduction to Amazon DynamoDB <ul style="list-style-type: none"> A. Create a new table B. Add data C. Modify existing items D. Query the table E. Delete the table 	13/07/2022	91-108
6	Introduction to Amazon Redshift <ul style="list-style-type: none"> 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 	03/08/2022	109-126

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

Practical 1: Getting Familiarized with AWS Console

A. Creating Aws Free Tier Account

B. Getting Familiarized with The Aws Console

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

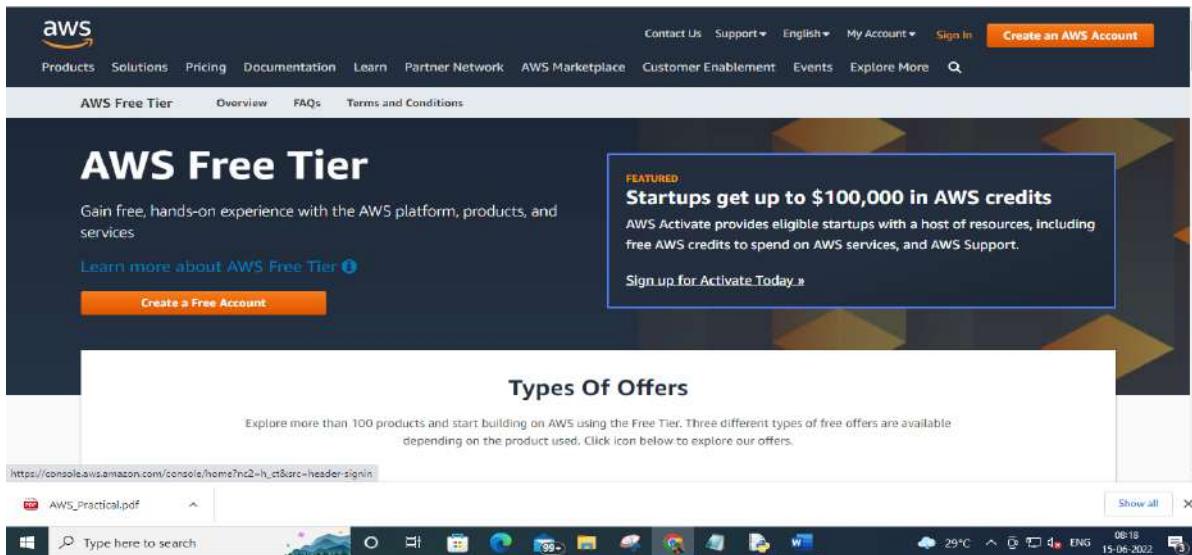
Creating an AWS Account is the first step you need to take in order to learn Amazon Web Services. Signing up for AWS provides you with all the tools you require to become an AWS professional.

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

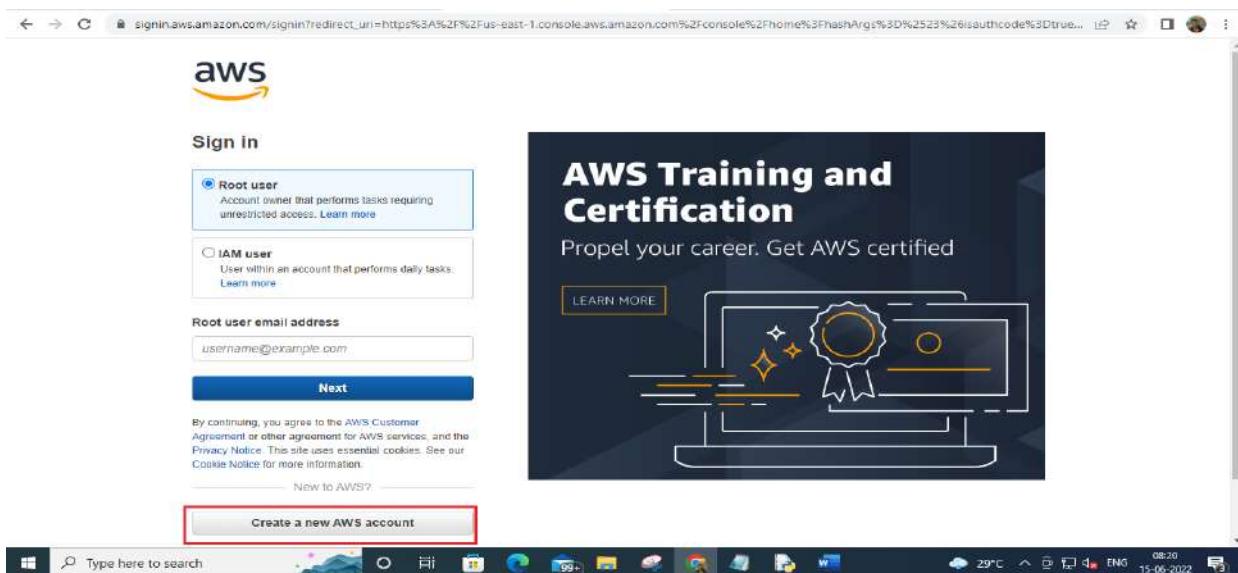
Step 1 – Visiting the Signup Page

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

You should see something like below:



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



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

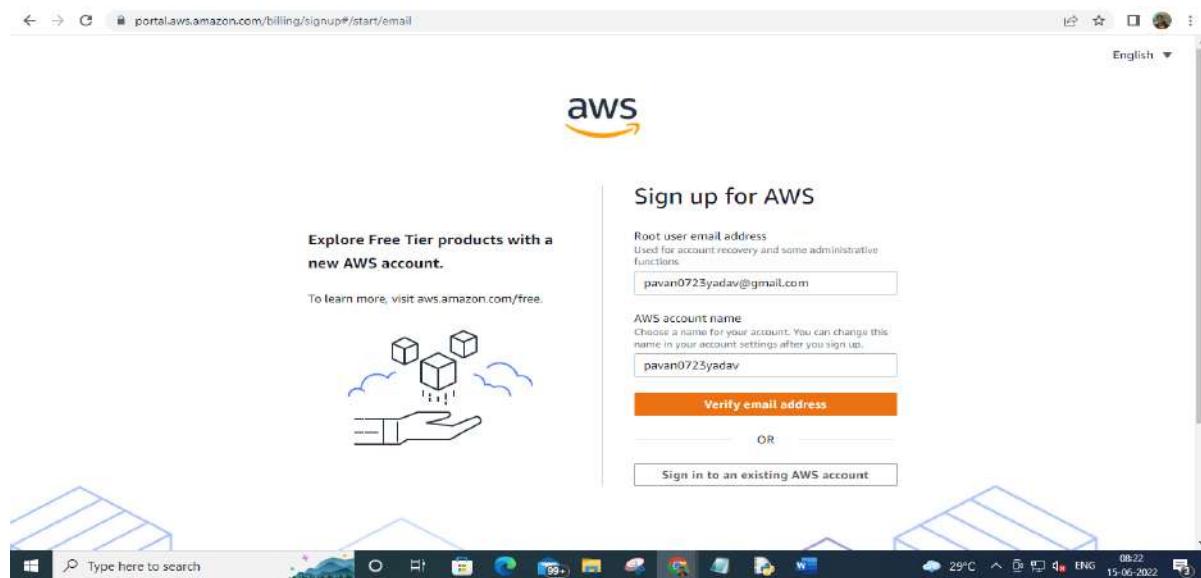
Step 2 – Entering User Details

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

Root user email address: pavan0723yadav@gmail.com

AWS account name: pavan0723yadav

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



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

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

Password: P@v@nK0723

Step 3 – Entering User Details

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

The screenshot shows the AWS sign-up process. 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, there's a "Sign up for AWS" form with sections for "Contact Information" and "How do you plan to use AWS?". The "Personal" radio button is selected. Below that, there are fields for "Full Name" (Pavan Yadav), "Phone Number" (843819799), and "Country or Region" (India).

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

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

Step 4 – Identity Confirmation

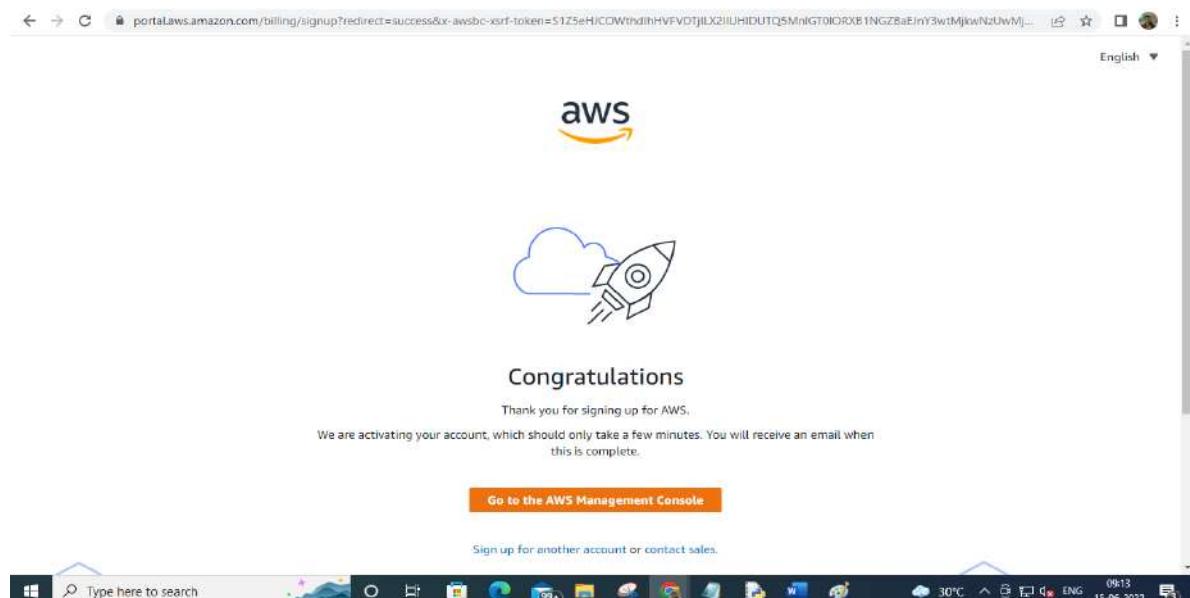
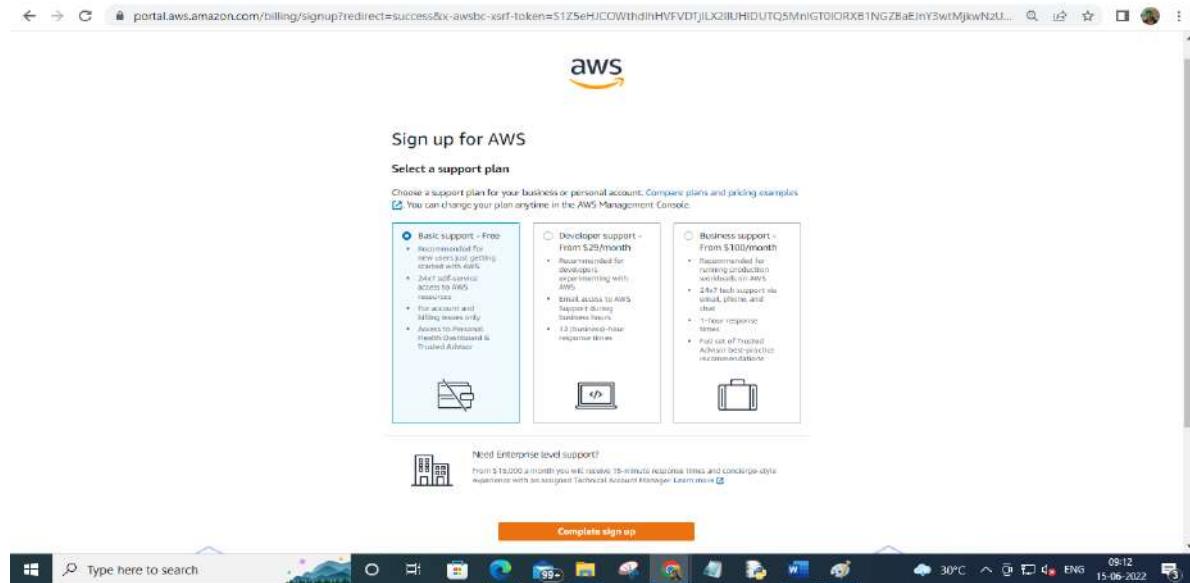
Once the credit card details are confirmed, you will need to complete the Identity Confirmation step. You will see the below screen:

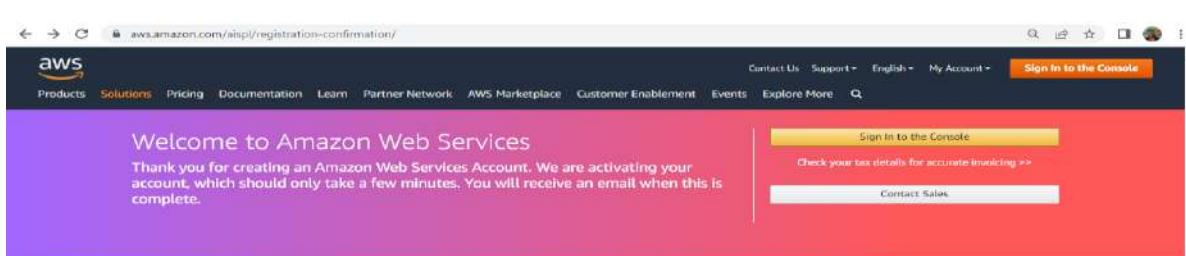
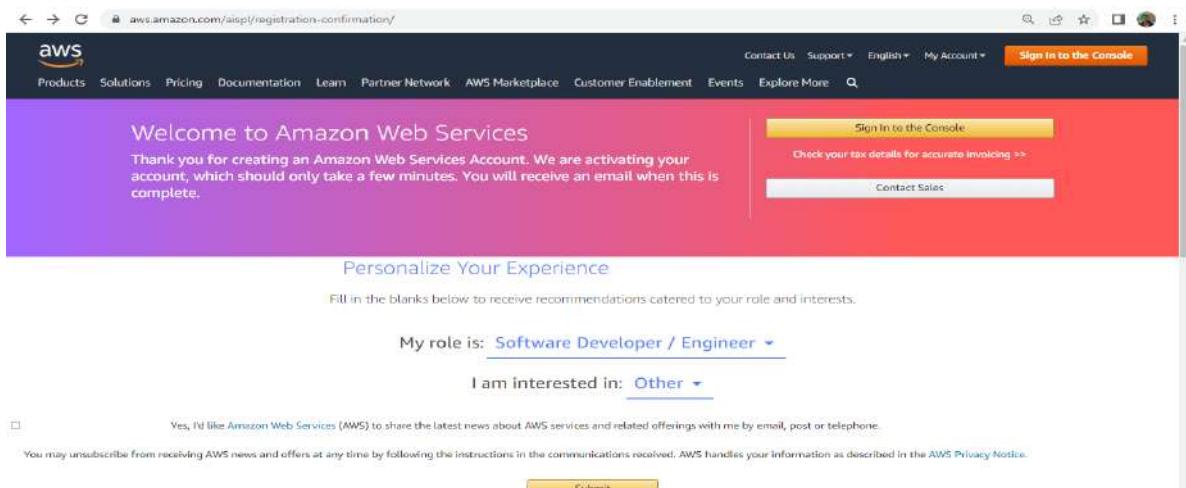
The screenshot shows the "Secure verification" and "Billing Information" steps. The "Secure verification" section contains a note about temporary hold on the card. The "Billing Information" section includes fields for "Credit or Debit card number" (ending in 2907), "Expiration date" (June 2026), "Cardholder's name" (Pavan Yadav), "CVV" (three asterisks), and "Billing address" (RJ College, Nearest Ghatkopar, Mumbai Maharashtra 400085). The "Use my contact address" radio button is selected.

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.





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 image consists of three vertically stacked screenshots of the AWS Console:

- Screenshot 1: AWS Console Home Page**
The 'Console Home' page features a 'Recently visited' section with a 'Support' link, and a 'Welcome to AWS' sidebar with links to 'Getting started with AWS', 'Training and certification', and 'What's new with AWS?'.
- Screenshot 2: EC2 Search Results**
A search for 'EC2' yields four results under 'Services': EC2 (Virtual Servers in the Cloud), EC2 Image Builder (A managed service to automate build, customize and deploy OS images), AWS Compute Optimizer (Recommend optimal AWS Compute resources for your workloads), and AWS Firewall Manager (Central management of firewall rules). A sidebar on the right provides links to 'Getting started with AWS', 'Training and certification', and 'What's new with AWS?'.
- Screenshot 3: Elastic IP Addresses**
The 'Elastic IP addresses' page shows a table with columns for Name, Allocated IPv4 add..., Type, Allocation ID, and Reverse DNS r. The table is currently empty. The left sidebar includes sections for EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Scheduled Instances, Capacity Reservations), and Images.

The screenshot shows the AWS EC2 Home page. The navigation bar at the top includes links for Services, Search, and AWS Lambda. The main content area has a sidebar with sections like EC2 Dashboard, Instances, and Images. The main panel displays the 'Zones' table:

Zone name	Zone ID
us-east-1a	use1-az4
us-east-1b	use1-az6
us-east-1c	use1-az1
us-east-1d	use1-az2
us-east-1e	use1-az3
us-east-1f	use1-az5

Other sections visible include 'Scheduled events' (No scheduled events), 'Migrate a server' (using AWS Application Migration Service), and 'Additional information' (Getting started guide, Documentation, All EC2 resources, Forums).

Navigation Bar

Navigation Pane

Select instance

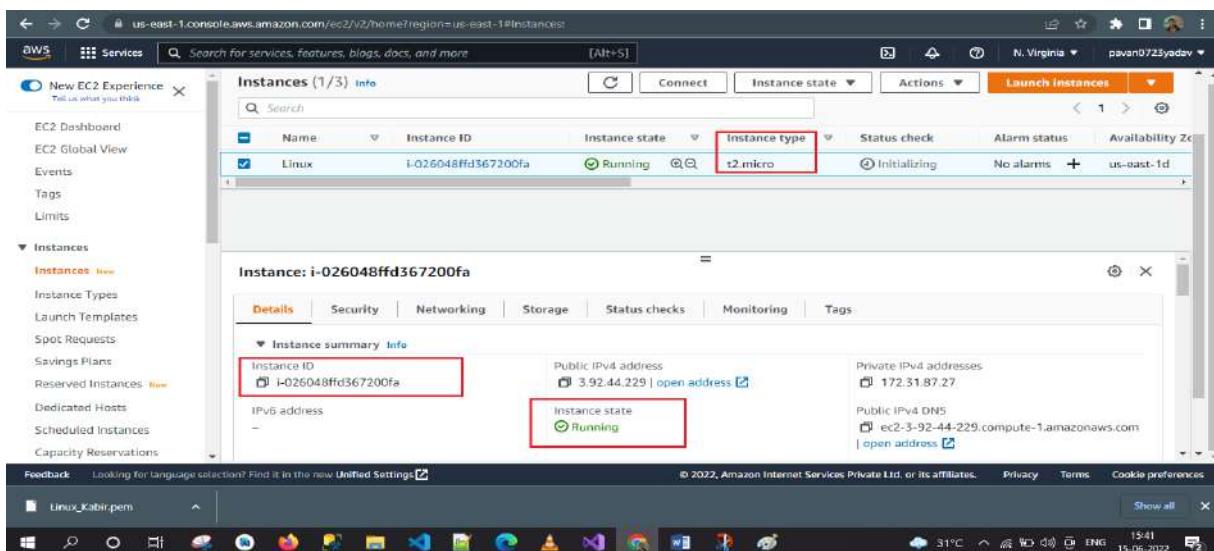
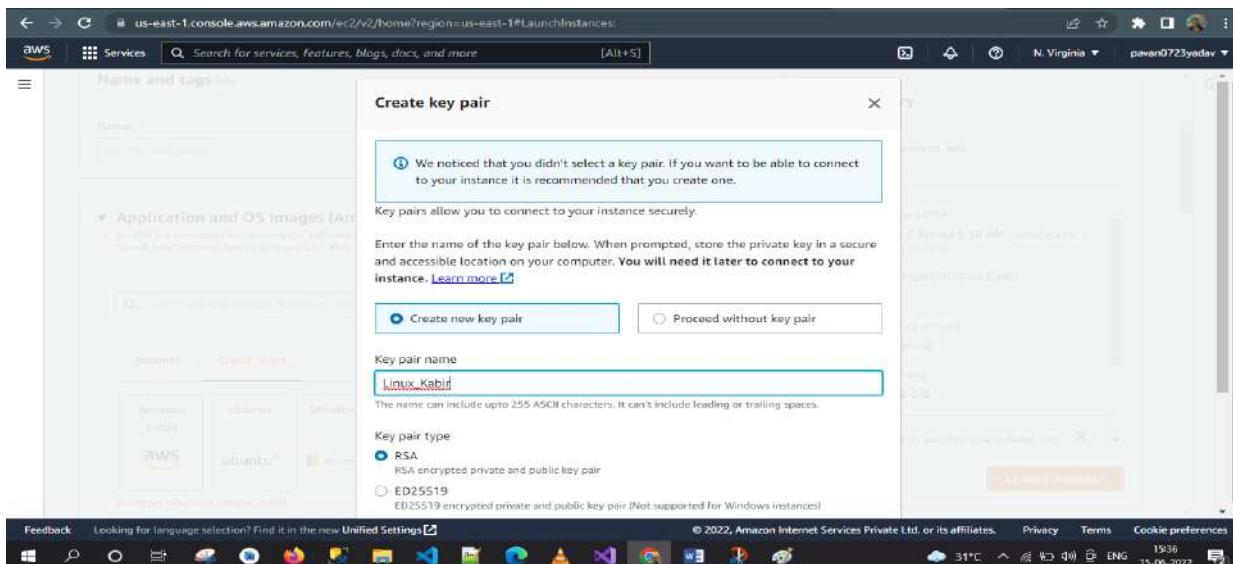
Zones

Region

The screenshot shows the AWS EC2 Resources page. The navigation bar at the top includes links for Services, Search, and AWS Lambda. The main content area has a sidebar with sections like EC2 Dashboard, Instances, and Images. The main panel displays the 'Resources' table:

Instances (running)	1	Dedicated Hosts	0
Elastic IPs	0	Instances	1
Key pairs	0	Load balancers	0
Placement groups	0	Security groups	2
Snapshots	0	Volumes	1

A callout box provides instructions for using the AWS Launch Wizard for Microsoft SQL Server Always On availability groups. The right side of the screen shows the 'Account attributes' and 'Explore AWS' sections.



1 Instance ID

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

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

2 Instance Status

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

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

System status checks

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

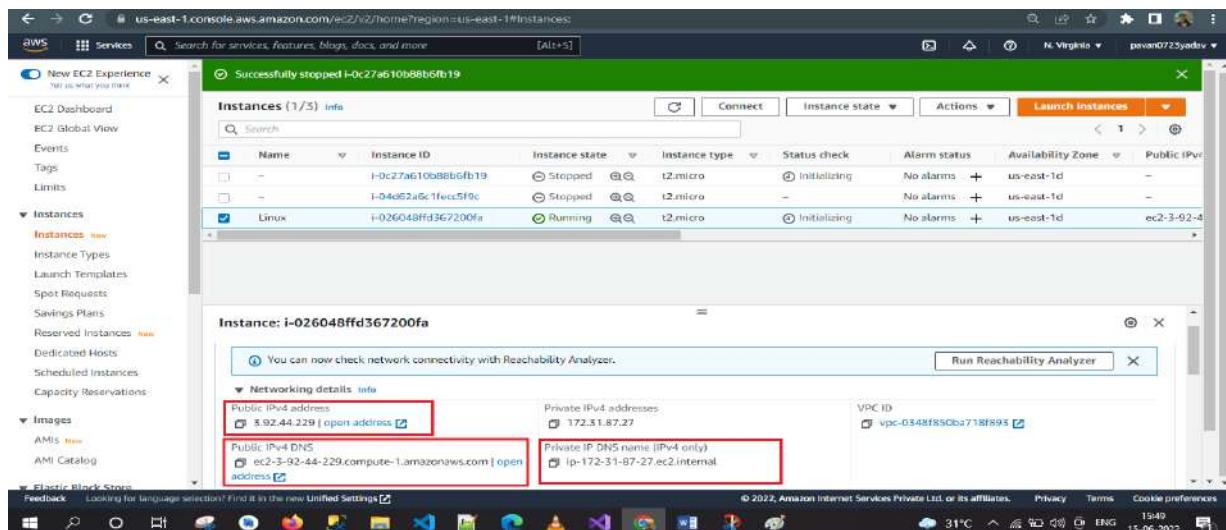
Instance status checks

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

3 Instance Type

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

Go to the Networking Tab



Public DNS

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

Private IP's

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

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

Go to Security Tab

The screenshot shows the AWS EC2 Instances page. A specific instance, "Linux" (ID: i-026048ffd367200fa), is selected and highlighted with a red border. The "Security groups" section for this instance shows it is associated with "sg-0ba31d8553361f8c5 (launch-wizard-3)". Below this, the "Inbound rules" section is expanded, also highlighted with a red border. It lists one rule: "sgr-0244c8e5fa54dbdf" with port range 22, protocol TCP, and source 0.0.0.0/0, which is associated with the same security group.

Security group rule ID	Port range	Protocol	Source	Security groups
sgr-0244c8e5fa54dbdf	22	TCP	0.0.0.0/0	launch-wizard-3

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

The screenshots show the AWS Qwiklabs interface for the 'Introduction to AWS Identity and Access Management (IAM)' lab. The first two screenshots are identical, showing the 'Start Lab' button, a timer at 00:45:00, and a sidebar with navigation links. The third screenshot shows the 'End Lab' button, a timer at 00:44:56, and the 'Open Console' button circled in red.

Screenshot 1 (Top):

- Start Lab button
- 00:45:00 timer
- I'm not a robot checkbox
- REDACTED IAM logo
- Introduction to AWS Identity and Access Management (IAM) title
- 45 minutes duration, Free, 5-star rating, AWS training and certification logo
- 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.
- 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, Additional Resources

Screenshot 2 (Middle):

- End Lab button
- 00:44:56 timer
- Cautions: 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 button (circled in red)
- Clipboard icon with ID: q15-48936904-7d79a807f1
- InstanceID: i-0776b46a22c0996d00
- AdministratorPassword: VXA95ewt17RXwCg
- Region: us-west-2
- Management (IAM) title
- 45 minutes duration, Free, 5-star rating, AWS training and certification logo
- 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.
- Note: Do not include any personal, identifying, or confidential information into the lab environment. Information entered may be visible to others.
- Corrections, feedback, or other questions? Contact us at [AWS Training and Certification](#)
- 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, Additional Resources

Screenshot 3 (Bottom):

- End Lab button
- 00:44:33 timer
- Cautions: 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 button (circled in red)
- Clipboard icon with ID: q15-48788863-8ab8c42c61
- InstanceID: i-036cc04ab988ecc6
- AdministratorPassword: 84bcPdfkB%tXY
- Region: us-west-2
- Introduction to AWS Identity and Access Management (IAM) title
- 45 minutes duration, Free, 5-star rating, Rate Lab, AWS training and certification logo
- 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.
- 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, Additional Resources

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 Home page. The Services menu on the left has 'IAM' highlighted with a red box. The main content area displays the 'Welcome to AWS' dashboard with sections for Getting started with AWS, Training and certification, and What's new with AWS. At the bottom, there are links for AWS Health, Cost and usage, and Feedback.

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

The screenshot shows the IAM Dashboard. The left navigation pane has 'User groups' expanded, with 'Users' selected and highlighted with a red box. The main content area shows the 'IAM dashboard' with sections for Security recommendations, IAM resources, and What's new. The IAM resources table shows 4 User groups, 5 Users, 18 Roles, and 0 Identity providers. On the right, there is an 'AWS Account' summary and a 'Tools' section.

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

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

The screenshot shows the AWS Identity and Access Management (IAM) service in the AWS Management Console. The left sidebar navigation bar includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (with 'User groups' and 'Users' selected), 'Roles', 'Policies', 'Identity providers', and 'Account settings'. Under 'Access reports', there are 'Access analyzer', 'Archive rules', 'Analyzers', and 'Settings'. The main content area is titled 'Users (5)' and contains a table with columns: User name, Groups, Last activity, MFA, Password a..., and Active. The table rows represent the users: 'awsstudent' (Group: GL ReadOnly, Last activity: Never, MFA: None, Active), 'root-qwkl' (Group: None, Last activity: Never, MFA: None, Active), 'user-1' (Group: None, Last activity: Never, MFA: None, Active), 'user-2' (Group: None, Last activity: Never, MFA: None, Active), and 'user-3' (Group: None, Last activity: Never, MFA: None, Active). A red box highlights the row for 'user-1'.

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

The screenshot shows the AWS IAM User summary page for 'user-1'. The left sidebar navigation bar is identical to the previous screenshot. The main content area displays the user's details: User ARN (arn:aws:iam::161361707178:user/spl66/user-1), Path (/spl66), and Creation time (2022-06-24 08:34 UTC+0530). Below this, there are tabs for 'Permissions', 'Groups', 'Tags (2)', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is active, showing a message: '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) with 'Add permissions' and 'Add inline policy' buttons. It also lists 'Permissions boundary (not set)' and 'Generate policy based on CloudTrail events'.

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

This screenshot is identical to the one above, showing the AWS IAM User summary page for 'user-1'. The user details, tabs, and 'Permissions' section all match the previous screenshot, confirming that user-1 has no permissions assigned.

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

The screenshot shows the AWS IAM User Summary page for a user named 'user-1'. The left navigation pane is open, showing various IAM management options like Dashboard, Access management, User groups, and Groups. The 'Groups' tab is highlighted with a red box. Below the tabs, there's a section for 'Attached permissions' which displays 'No results'.

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

The screenshot shows the AWS IAM User Summary page for 'user-1'. The 'Security credentials' tab is selected, highlighted with a red box. Under the 'Sign-in credentials' section, the 'Console password' status is shown as 'Enabled (never signed in) | Manage', also highlighted with a red box.

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 AWS IAM User Groups page. The left sidebar has 'User groups' selected. The main table lists four user groups:

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	10 minutes ago
EC2-Support	0	Defined	10 minutes ago
GLReadonly	1	Defined	10 minutes ago
S3-Support	0	Defined	10 minutes ago

Step 11 – Click the EC2-Support group.

The screenshot shows the AWS IAM User Groups - EC2-Support summary page. The left sidebar has 'User groups' selected. The main section shows the EC2-Support group details and its users. The 'Permissions' tab is highlighted with a red box.

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

Step 12 – Click the Permissions tab.

The screenshot shows the AWS IAM User Groups - EC2-Support permissions page. The left sidebar has 'User groups' selected. The main section shows the EC2-Support group details and its permissions. The 'Permissions' tab is highlighted with a red box. A specific policy, 'AmazonEC2ReadOnlyAccess', is highlighted with a red box.

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 13 – Under Actions, click the Show Policy link.

```

{
    "Version": "2012-12-01",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:Describe",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:Describe",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:ListMetrics",
                "CloudWatchMetricsDescribe",
                "CloudWatchMetricsListMetrics"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "autoscaling:Describe",
            "Resource": "*"
        }
    ]
}
  
```

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 AWS IAM Groups page. On the left, the navigation pane is open under 'Access management' with 'User groups' selected. The main area displays the 'EC2-Support' user group. The 'Permissions' tab is active, showing one policy attached: 'AmazonEC2ReadOnlyAccess'. The ARN of the group is listed as arn:aws:iam:723548672068:group/spl66/EC2-Support.

Policy name	Type	Description
AmazonEC2ReadOnlyAccess	AWS managed	Provides read only access to

Step 15 – Click the S3-Support Group.

The screenshot shows the AWS IAM User Groups page. The 'S3-Support' group is highlighted with a red box. The table lists four user groups: EC2-Admin, EC2-Support, QLReadOnly, and S3-Support.

Group name	Users	Permissions	Creation time
EC2-Admin	>Loading	>Loading	4 minutes ago
EC2-Support	⚠ 0	>Loading	4 minutes ago
QLReadOnly	>Loading	>Loading	4 minutes ago
S3-Support	>Loading	>Loading	4 minutes ago

The S3-Support group has the AmazonS3ReadOnlyAccess policy attached.

The screenshot shows the AWS IAM console with the 'User groups' section selected. A user group named 'S3-Support' is displayed, which was created on June 22, 2022, at 08:34 (UTC+05:30). The ARN for this group is arn:aws:iam::901517298687:group/spi66/S3-Support. The 'Permissions' tab is active, showing one managed policy named 'AmazonS3ReadOnlyAccess' attached to the group. This policy provides read-only access to all buckets via the AWS Management Console. The policy document is shown in JSON format:

```

1 = [
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:Get*",
8         "s3:List*",
9         "s3:Object-Lambda:Get*",
10        "s3:Object-Lambda:List*"
11      ],
12      "Resource": "*"
13    }
14  ]
15 ]

```

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

The screenshot shows the 'Show Policy' window for the 'AmazonS3ReadOnlyAccess' policy. The policy document is displayed in JSON format, with the 'Resource' section highlighted by a red box. The policy allows actions like 's3:Get*' and 's3:List*' on all resources ('*').

```

1 = [
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:Get*",
8         "s3:List*",
9         "s3:Object-Lambda:Get*",
10        "s3:Object-Lambda:List*"
11      ],
12      "Resource": "*"
13    }
14  ]
15 ]

```

Step 17 – Close the Show Policy window.

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

S3-Support Group Summary

User group name	Creation time	ARN
S3-Support	June 24, 2022, 16:43 (UTC+05:30)	arn:aws:iam:723548672068:group/s3-Support

Permissions policies (1) Info
You can attach up to 10 managed policies.

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

Step 19 – Click the EC2-Admin group

User groups (4) Info
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time
EC2-Admin	Loading	Loading	7 minutes ago
EC2-Support	⚠ 0	Loading	7 minutes ago
QLReadOnly	>Loading	>Loading	7 minutes ago
S3-Support	⚠ 0	>Loading	7 minutes ago

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 Permissions page. The 'Permissions' tab is selected. A policy named 'EC2-Admin-Policy' is listed. The JSON code for the policy is displayed:

```

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.        "Effect": "Allow"
12.    }
13. ]

```

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 AWS IAM Policy Editor for the 'Edit EC2-Admin-Policy' step. The policy is defined using the visual editor. It includes actions for EC2 (136 actions) and CloudWatch (1 action). The 'Review policy' button is highlighted at the bottom right.

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:

- user-1 -> S3-Support Read-Only -> access to Amazon S3
- user-2 -> EC2-Support Read-Only -> access to Amazon EC2
- 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

User group name	Creation time	ARN
EC2-Admin	June 28, 2022, 16:43 (UTC+06:30)	arn:aws:iam:723548672068:group/policy/EC2-Admin

Step 23 – Click the S3-Support group.

Group name	Users	Permissions	Creation time
EC2-Admin	0	Loading	12 minutes ago
EC2-Support	0	Loading	12 minutes ago
QLReadOnly	0	Loading	12 minutes ago
S3-Support	0	Loading	12 minutes ago

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

The screenshot shows the AWS IAM User Groups page for the 'S3-Support' group. The 'Users' tab is selected. At the top right of the user list table, there is a red box around the 'Add users' button. The user list table shows one entry: 'User name: awstudent'. Below the table, a message says 'No resources to display'.

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 'Add users to S3-Support' dialog box. The 'user-1' checkbox is checked. At the bottom right of the dialog box, there is a red box around the 'Add users' button.

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

Screenshot of the AWS IAM User Groups page for the S3-Support group. The 'Users added to this group' section is highlighted with a red box. Below it, the 'user-1' entry in the 'User name' column of the table is also highlighted with a red box.

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.

Screenshot of the AWS IAM User Groups page for the EC2-Support group. The 'Users added to this group' section is highlighted with a red box. Below it, the 'user-2' entry in the 'User name' column of the table is also highlighted with a red box.

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.

The screenshot shows the AWS IAM User Groups page for the 'EC2-Admin' group. The 'Users' tab is selected, showing a single user entry:

User name	Groups	Last activity	Creation time
user-3		None	17 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.

The screenshot shows the AWS IAM User Groups page for the 'EC2-Admin' group. The 'Users' tab is selected, showing a single user entry:

User name	Groups	Last activity	Creation time
user-3		None	17 minutes ago

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

The screenshot shows the AWS IAM Groups page. On the left, there's a navigation pane with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'User groups' is highlighted. The main area displays a table titled 'User groups (4) Info'. The table has columns for 'Group name', 'Users', 'Permissions', and 'Creation time'. Each row shows a group name with a user count of 1, followed by 'Loading' under 'Permissions' and a timestamp like '18 minutes ago' under 'Creation time'. At the top right of the table, there are 'Delete' and 'Create group' buttons. Below the table is a search bar and a message about user groups. The bottom of the screen shows the standard AWS footer with various service icons and the date/time.

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

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

Task 3: Sign-In and Test Users

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

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

The screenshot shows the AWS IAM Dashboard. On the left, the navigation pane has 'Dashboard' selected. The main area features a 'Security recommendations' section with a red warning icon and a link to add MFA for the root user. Below it is the 'IAM resources' section, which includes a table with counts for User groups (4), Users (5), Roles (18), Policies (2), and Identity providers (0). To the right, there's an 'AWS Account' summary with fields for Account ID (723548672068), Account Alias (723548672068), and a sign-in URL. There are also 'Tools' sections for 'Policy simulator' and 'Web identity federation playground'. The bottom of the screen shows the standard AWS footer.

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

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

The screenshot shows the AWS IAM Dashboard. In the top right corner, there is a red box highlighting the "AWS Account" section which displays the Account ID (723548672068) and Account Alias (723548672068). Below this, a message says "Sign in URL Copied" with the URL "https://723548672068signin.aws.amazon.com/console".

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

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

The screenshot shows the AWS IAM Dashboard with a "Notepad" application window overlaid. The Notepad window has the title "Untitled - Notepad" and contains the URL "https://723548672068signin.aws.amazon.com/console". This indicates that the sign-in URL has been copied from the AWS dashboard and pasted into the Notepad.

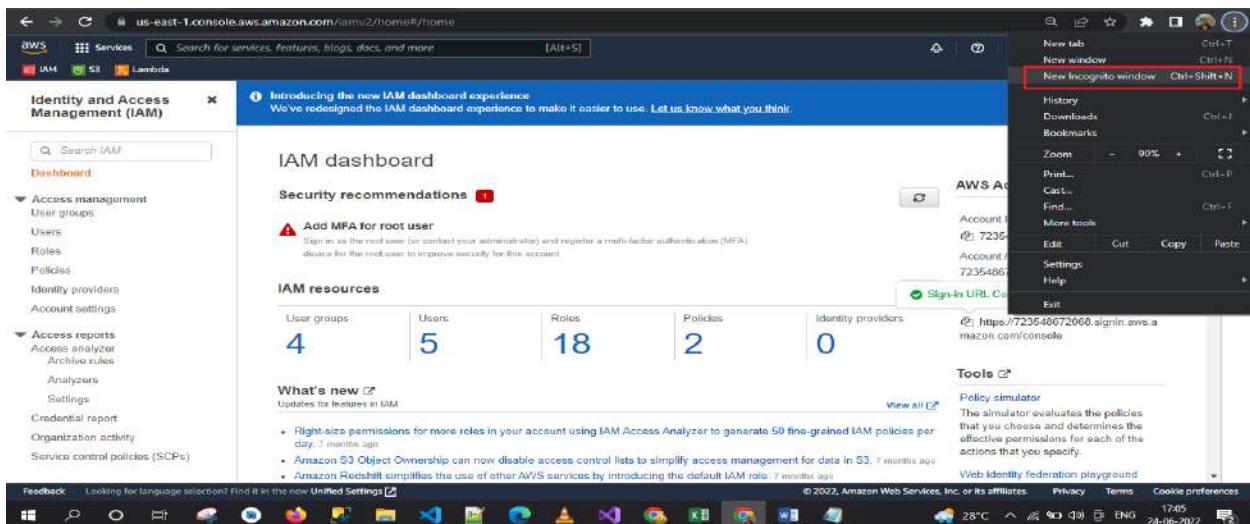
Step 31 – Open a private window.

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



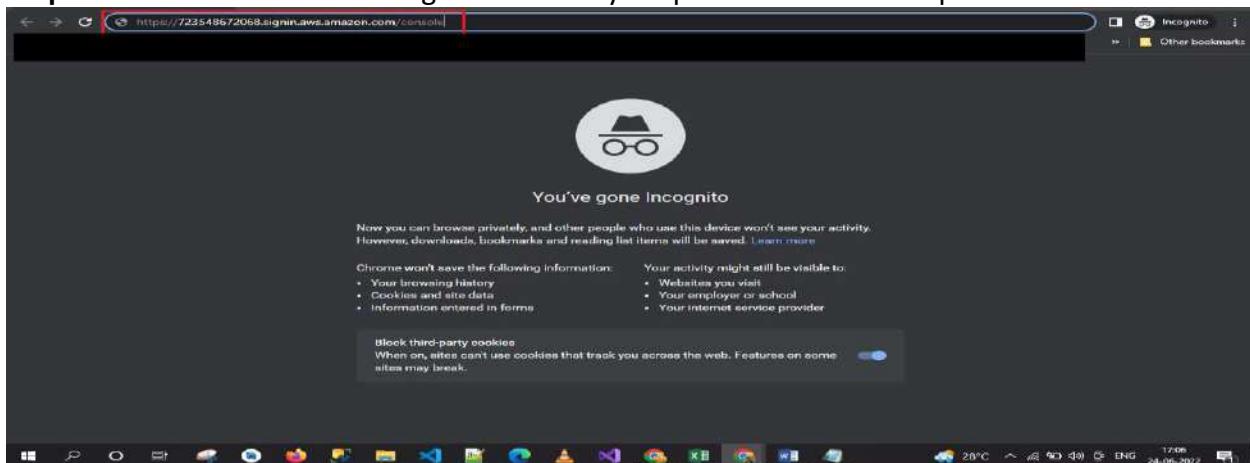
Microsoft Edge

- 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.

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.

AdministratorAccess

Open Console

q3x-48962291-5ed5d4a9-f1

Instances

1-U54424F7d52deb712

AdministratorAccess

1-xPPfH880c5hx

Region

us-west-2

End Lab 00:22:38

Introduction to AWS Identity and Access Management (IAM)

45 minutes Free 4.5 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

Sign in as IAM user

Account ID (12 digits) or account alias

723548672068

IAM user name

user-1

Password

Remember this account

Sign in

Sign in using root user email

Forgot password?

AWS DeepRacer offers online, in-person, and hybrid events for getting started with machine learning

Learn more

English

The new AWS Console Home will replace your existing experience soon. Starting June 2022, the new AWS Console Home will replace your current experience. Switch now to customize your Console Home and view valuable insights. Learn more or tell us what you think.

AWS Management Console

New AWS Console Home

Switch now

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.

AWS services

Recently visited services

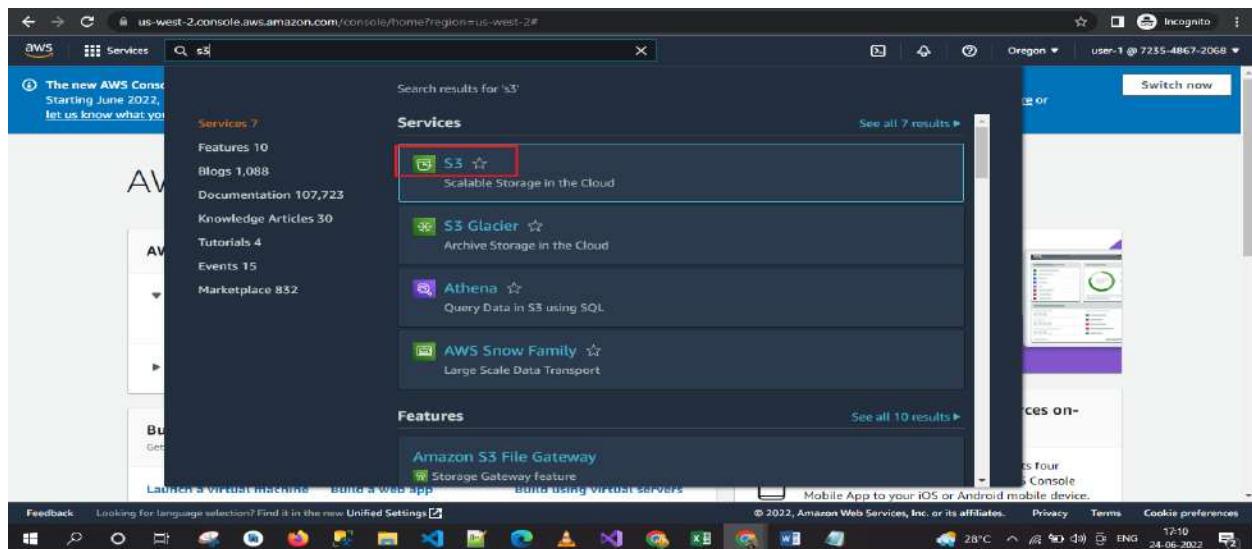
EC2 S3

All services

Build a solution

Launch a virtual machine Build a web app Build using virtual servers

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 'Buckets' page in the AWS S3 console. It displays three buckets: 'ql-cf-templates-1656069215-34d8952c15380165-us-west-2', 'qls-48962291-Sed584a9f8c86350-s3bucket-1af1gf1cf1pu13', and 'ql-trail-lab-4154-1656069219'. The third bucket is highlighted with a red box. The status bar at the bottom indicates it's a Microsoft Windows environment.

The screenshot shows the 'Objects' page for the selected bucket 'ql-trail-lab-4154-1656069219'. It lists one object, 'lab-4154.json', which is highlighted with a red box. The status bar at the bottom indicates it's a Microsoft Windows environment.

The screenshot shows the AWS S3 console with the file 'lab-4134.json' selected. The 'Permissions' tab is active. The 'Access control list (ACL)' table includes the following rows:

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: 06856038f13768b1b092d1a9b4d5e28d7aa7e899b988424a64b930548928c85d	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.

The screenshot shows the AWS Services menu search results for 'ec2'. The 'EC2' service is highlighted with a red box. Other services listed include EC2 Image Builder, AWS Compute Optimizer, and AWS Firewall Manager.

Login with new password and redo all the steps.

Step 38 – 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

The screenshot shows the AWS EC2 Global View interface. On the left, a navigation pane includes links for EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances (with a red box around 'Instances'), and Images. The main area displays a grid of resources categorized by region: US East (N. Virginia), US East (Ohio), US West (N. California), US West (Oregon) (highlighted in orange), Africa (Cape Town), Asia Pacific (Hong Kong), Asia Pacific (Jakarta), Asia Pacific (Mumbai), Asia Pacific (Osaka), Asia Pacific (Seoul), Asia Pacific (Singapore), and Asia Pacific (Tokyo). Each row contains links for Instances (running), Elastic IPs, Key pairs, Placement groups, Snapshots, Dedicated Hosts, Load balancers, Security groups, and Volumes. A message at the bottom encourages users to learn more about Microsoft SQL Server Always On availability groups.

The screenshot shows the AWS IAM training lab interface. At the top, it says 'Introduction to AWS Identity and Access Management (IAM)' with a timer of '00:12:33'. Below this, there's a 'Caution' note about not deviating from instructions. The main content area features the 'aws training and certification' logo and information about the SPL-66 - version 3.1.14 lab, which is 45 minutes long and free. It includes a 'Rate Lab' button and a note about copyright. To the right is a sidebar with links for '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'. The bottom of the screen shows a Windows taskbar with various icons.

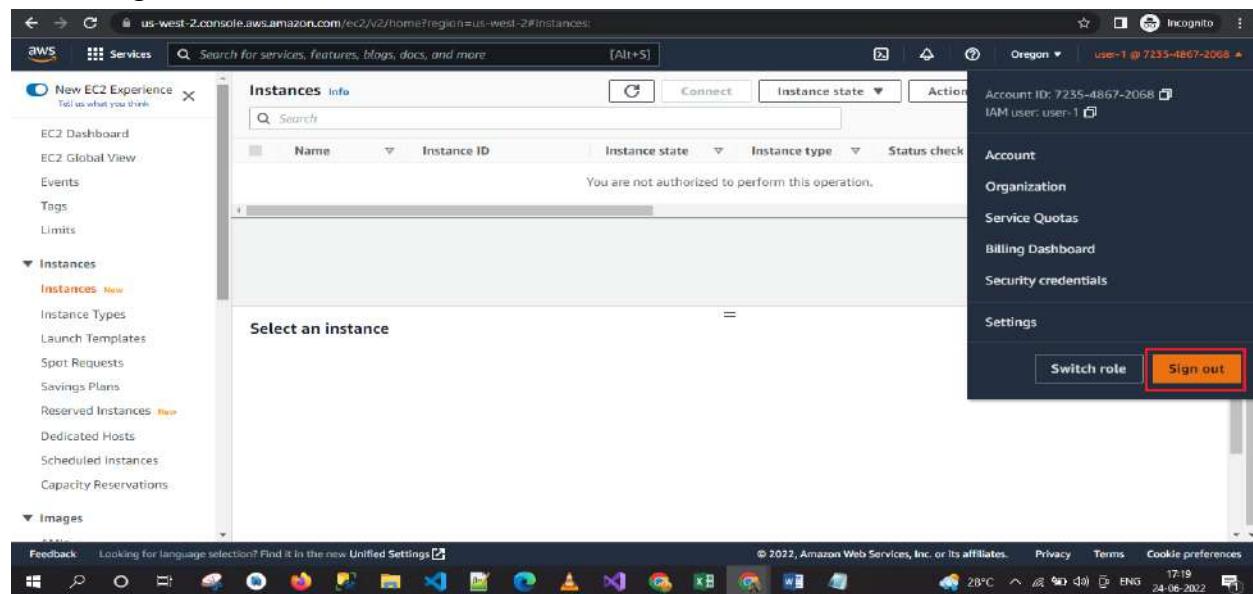
Step 39 – In the left navigation pane, click Instances.

The screenshot shows the AWS EC2 Instances page. The left navigation pane has a red box around the 'Instances' link under the 'Instances' section. The main content area shows a table with columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Availability Z. A message box in the center states 'You are not authorized to perform this operation.' The bottom of the screen shows a Windows taskbar.

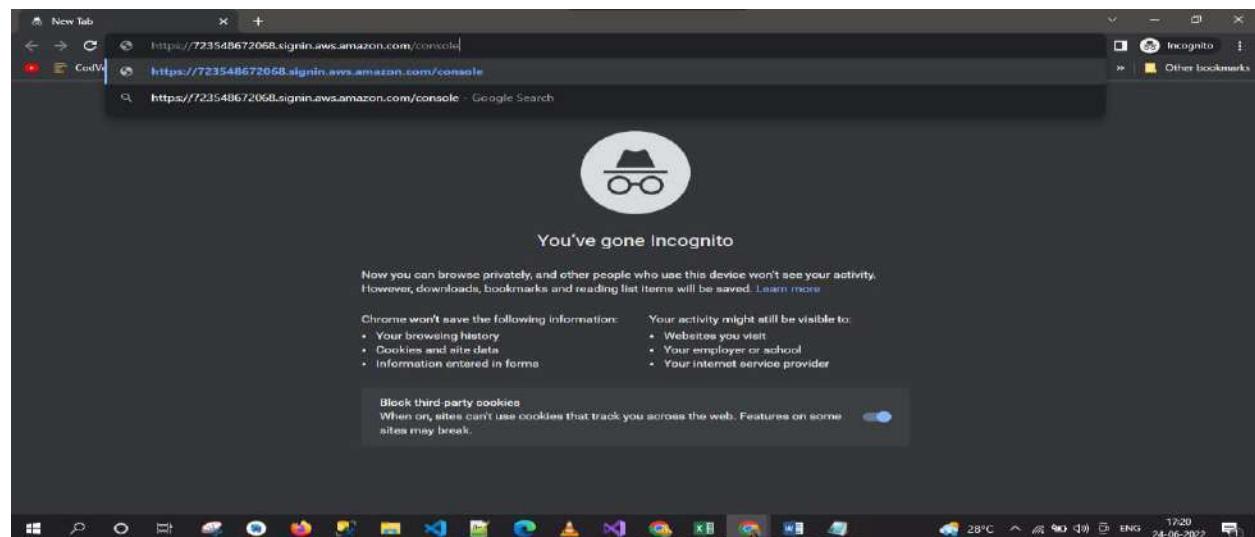
You cannot see any instances! Instead, it says an error occurred fetching instance data: You are not authorized to perform this operation... This is because your user has not been assigned any permissions to use Amazon EC2. You will now sign-in as user-2, who has been hired as your Amazon EC2 support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

Step 40 – Sign user-1 out of the AWS Management Console by configuring the following:

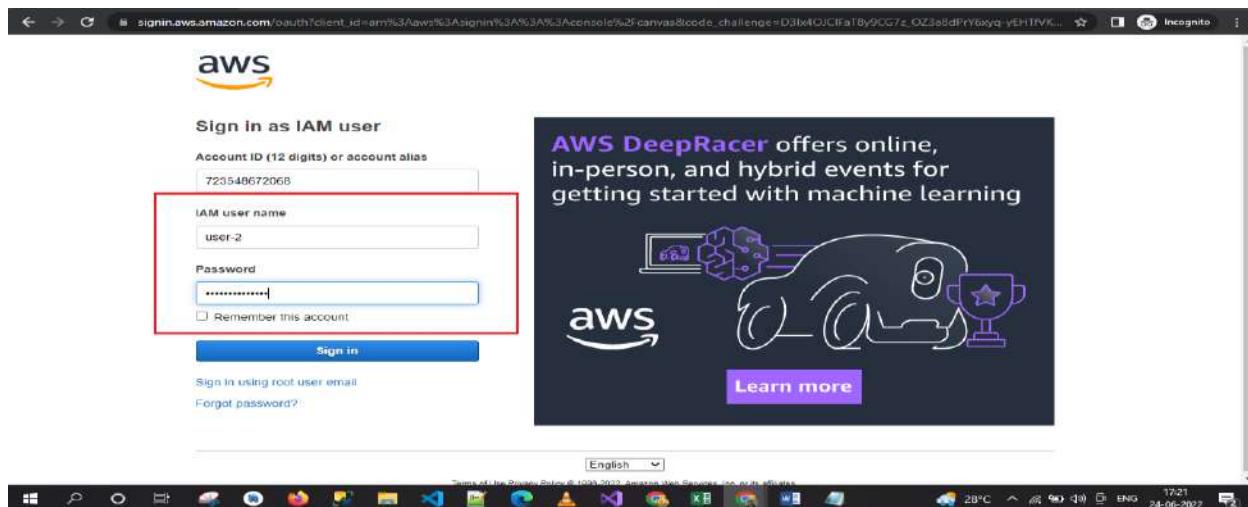
- At the top of the screen, click user-1
- Click Sign Out



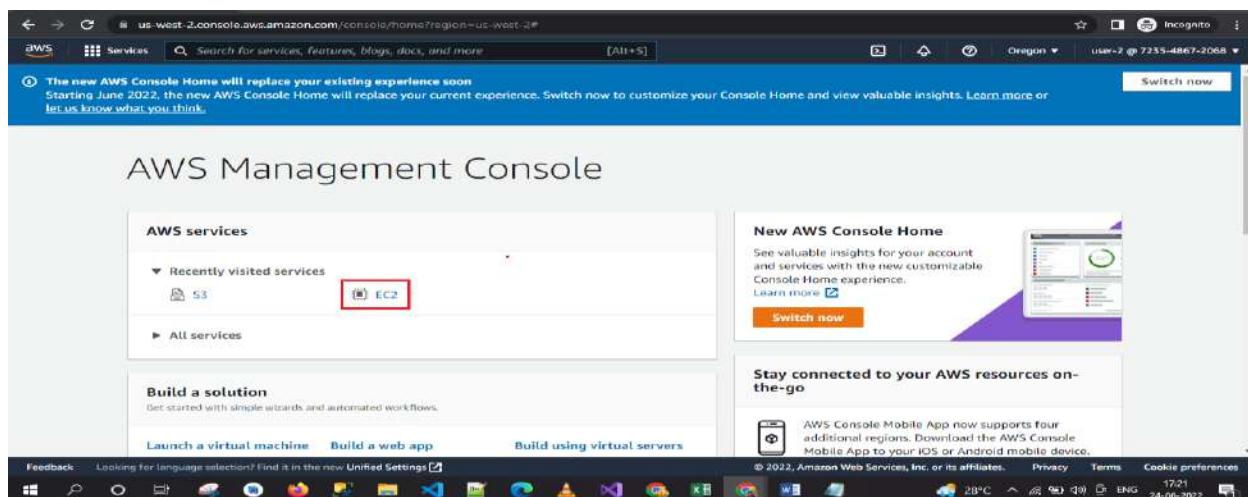
Step 41 – Paste the IAM users sign-in link into your private window and press Enter. This links should be in your text editor.



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

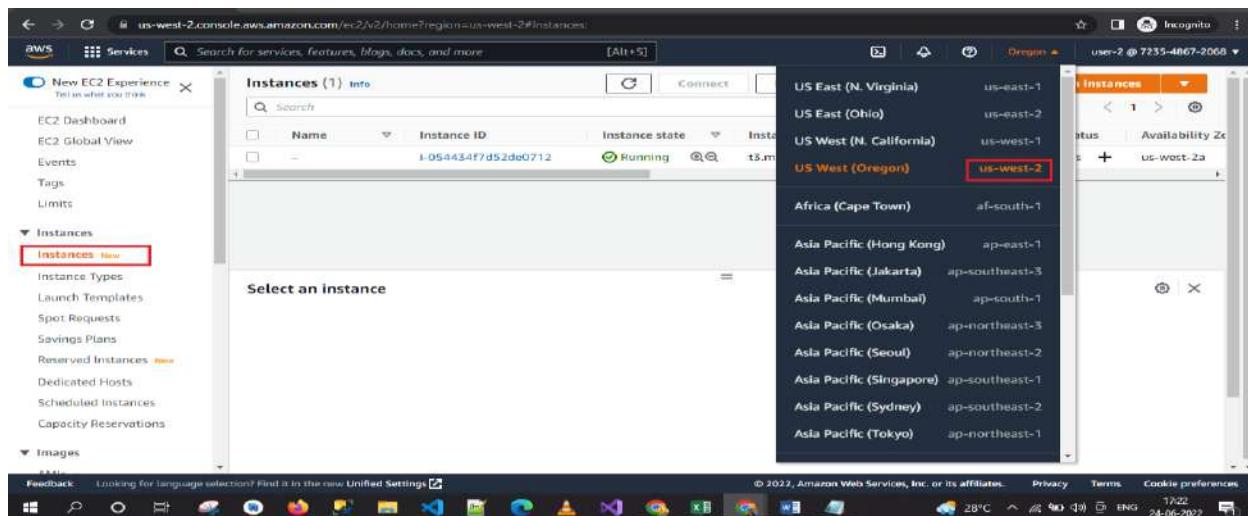


Step 43 – In the Services menu, click EC2.



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



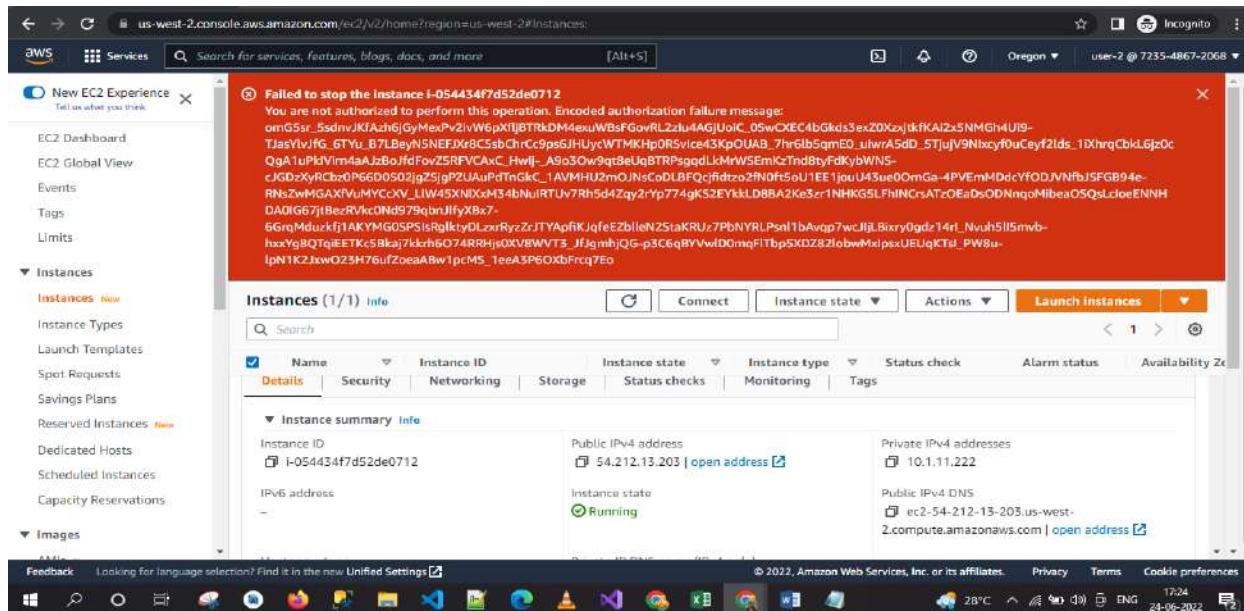
Step 45 – You are now able to see an Amazon EC2 instance because you have Read Only permissions. However, you will not be able to make any changes to Amazon EC2 resources.

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

The screenshot shows the AWS EC2 Instances page. A single instance, 'i-054434f7d52de0712', is listed as 'Running' with the instance type 't5.micro'. The 'Actions' menu for this instance is open, with the 'Stop instance' option highlighted. The instance details panel shows its public IPv4 address (54.212.13.203) and private IP (10.1.1.222). The status checks indicate 2/2 checks passed. The page also includes tabs for Details, Security, Metrics, and Instance summary info.

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

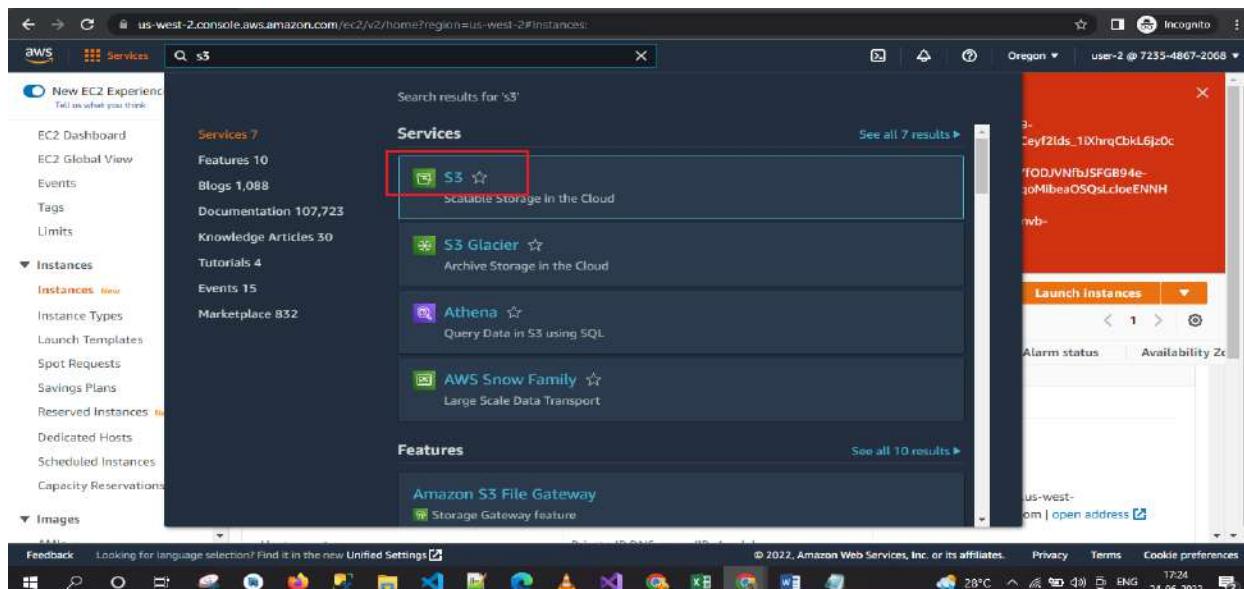
The screenshot shows the same AWS EC2 Instances page as before, but with a modal dialog box titled 'Stop instance?'. The dialog lists the instance ID 'i-054434f7d52de0712' and contains the instruction 'To confirm that you want to stop the instance, choose the Stop button below.' There are 'Cancel' and 'Stop' buttons at the bottom of the dialog. The background page remains largely the same, showing the instance details and status.



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



The screenshot shows the AWS S3 console with a message: "You don't have permissions to list buckets". This indicates that the user lacks the necessary permissions to view their own buckets.

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:

- At the top of the screen, click user-2.
- Click Sign Out.

The screenshot shows the AWS S3 console with the "Sign out" button highlighted in a red box. The user's account information is also visible in the top right corner.

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.

The screenshot shows the AWS Management Console homepage. In the top left, under 'AWS services', there's a list of recently visited services, with 'EC2' highlighted by a red box. To the right, there's a promotional banner for the 'New AWS Console Home', which promises valuable insights and a customizable experience. Below the banner, there are sections for 'Build a solution', 'Launch a virtual machine', 'Build a web app', and 'Build using virtual servers'. At the bottom of the page, there's a feedback link and a footer with copyright information and links to privacy, terms, and cookie preferences.

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

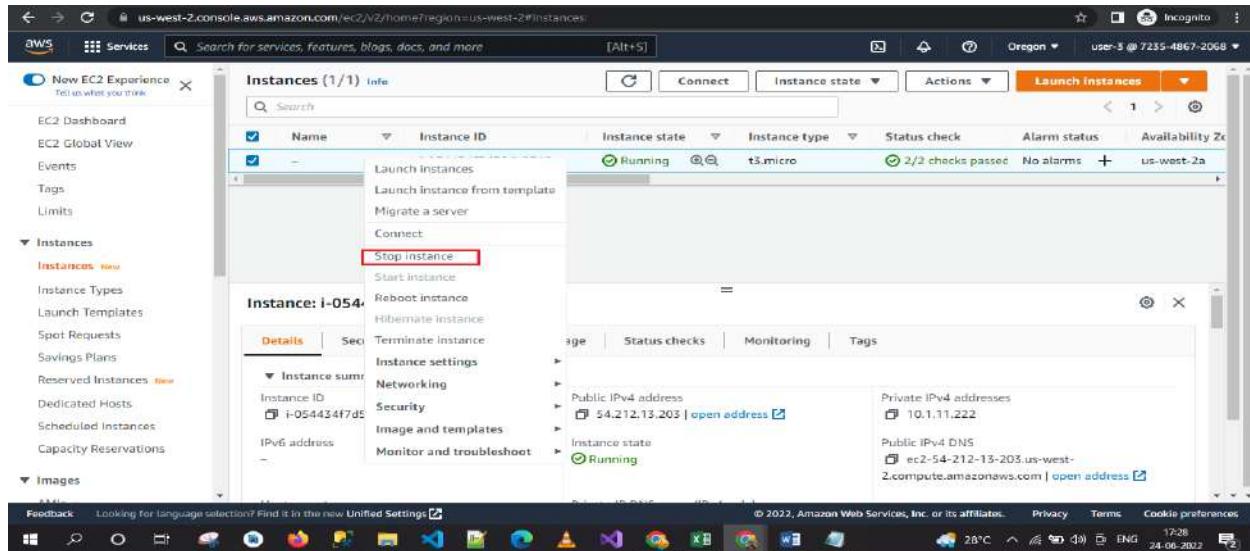
- Clicking the drop-down arrow at the top of the screen, to the left of Support
 - Selecting the region value that matches the value of Region to the left of these instructions
- Step 55** – In the navigation pane on the left, click Instances.

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 the AWS EC2 Instances page. On the left, there's a navigation pane with options like 'EC2 Dashboard', 'Events', 'Tags', 'Limits', 'Instances' (which is selected), 'Images', and 'Snapshots'. The main area displays a table titled 'Instances (1/1)'. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Availability Zone. One instance is listed: 'i-054434f7d52de0712' (Name), 'i-054434f7d52de0712' (Instance ID), 'Running' (Instance state), 't3.micro' (Instance type), '2/2 checks passed' (Status check), 'No alarms' (Alarm status), and 'us-west-2a' (Availability Zone). Below the table, there's a detailed view for the selected instance, showing its summary, security group, networking, storage, status checks, monitoring, and tags. The instance summary shows the Public IPv4 address as 54.212.13.203 and the Private IPv4 address as 10.11.22.2.

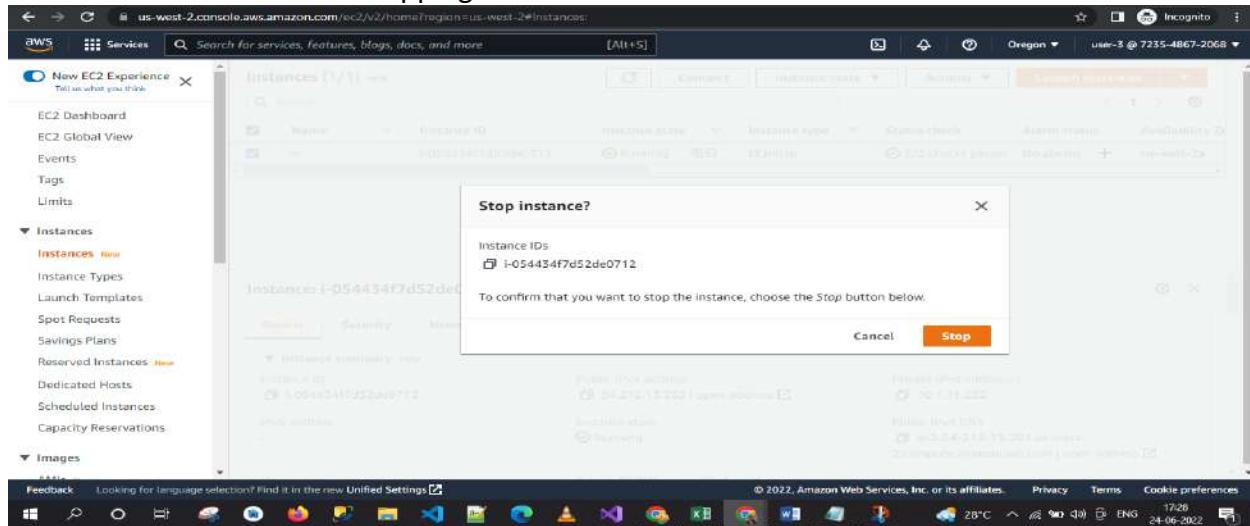
Step 56 – In the Actions menu, click Instance State > Stop

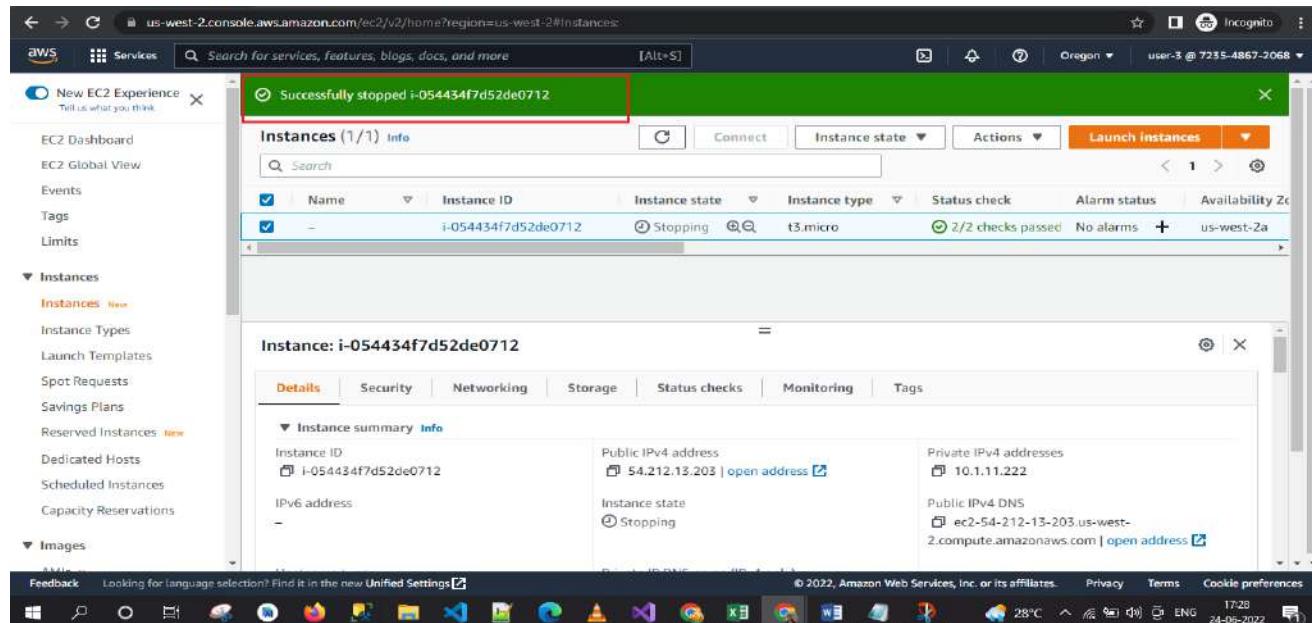
Right Click on the Instance and Click on the Stop instance



Step 57 – In the Stop Instances window, click Yes, Stop.

The instance will enter the stopping state and will shut down.





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

The screenshot shows the AWS Qwiklabs 'Introduction to AWS Identity and Access Management (IAM)' lab. The page includes a timer at 00:00:27, a red 'End Lab' button, and a note about not deviating from instructions. It also displays session details like S3 bucket, instance ID, administrator password, and region. To the right, a 'Lab Overview' section provides an introduction to IAM, listing tasks such as 'Explore the Users and Groups', 'Add Users to Groups', 'Sign-In and Test Users', and 'Conclusion'. The taskbar at the bottom shows various application icons.

Step 59 –Return to the AWS Management Console.

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

Practical 3: Working with S3 Buckets

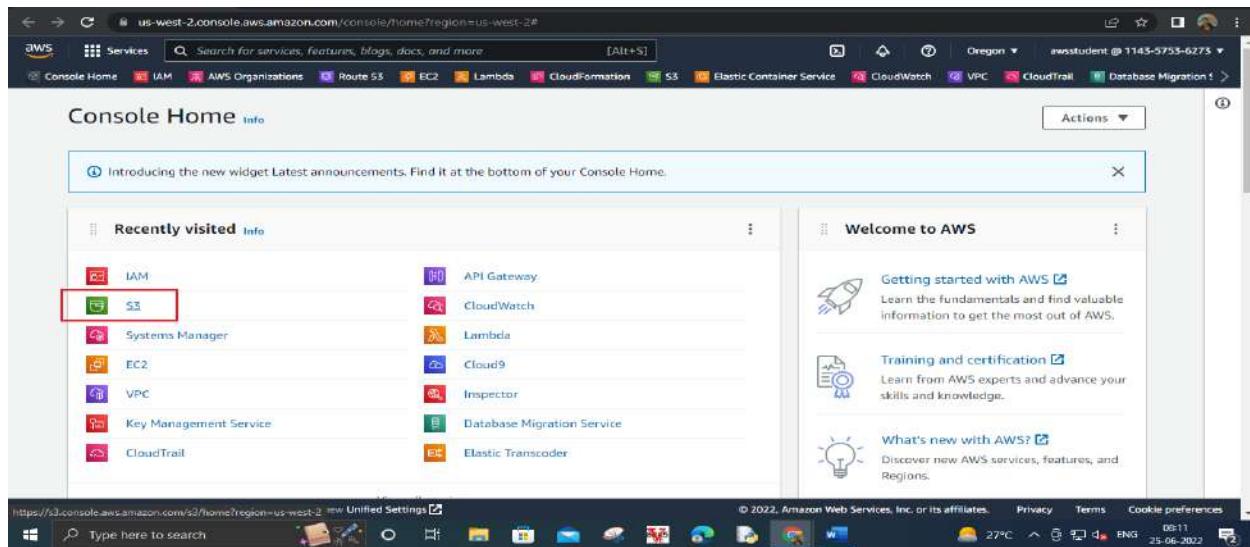
- A. Create a Bucket**
- B. Upload an object to the bucket**
- C. Make an Object public**
- D. Create a bucket policy**
- E. Explore versioning**

Task 1: Create a bucket

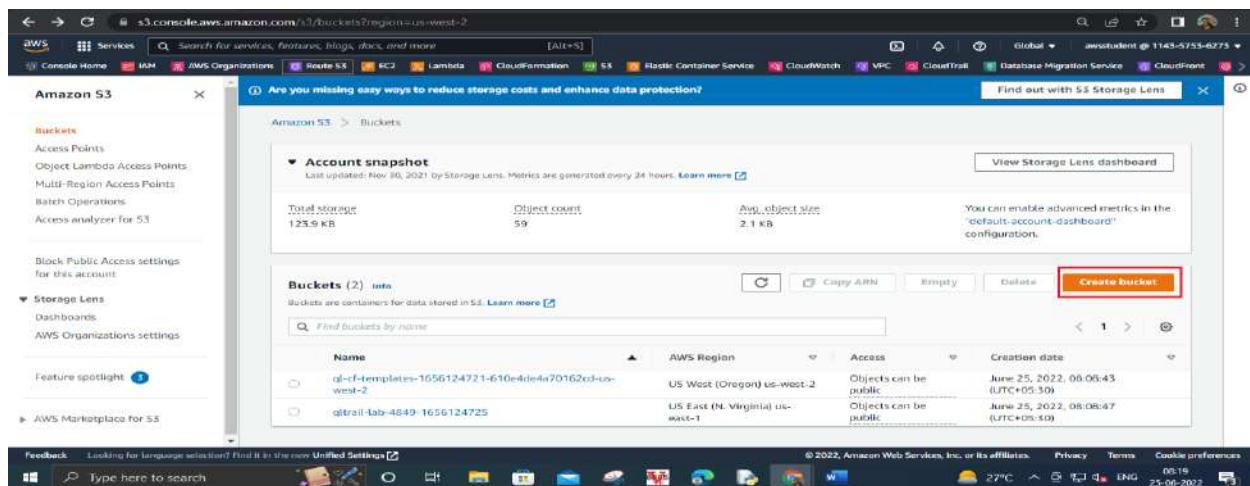
Step 1 –Click Start Lab

Step 2 – Click on Open Console

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



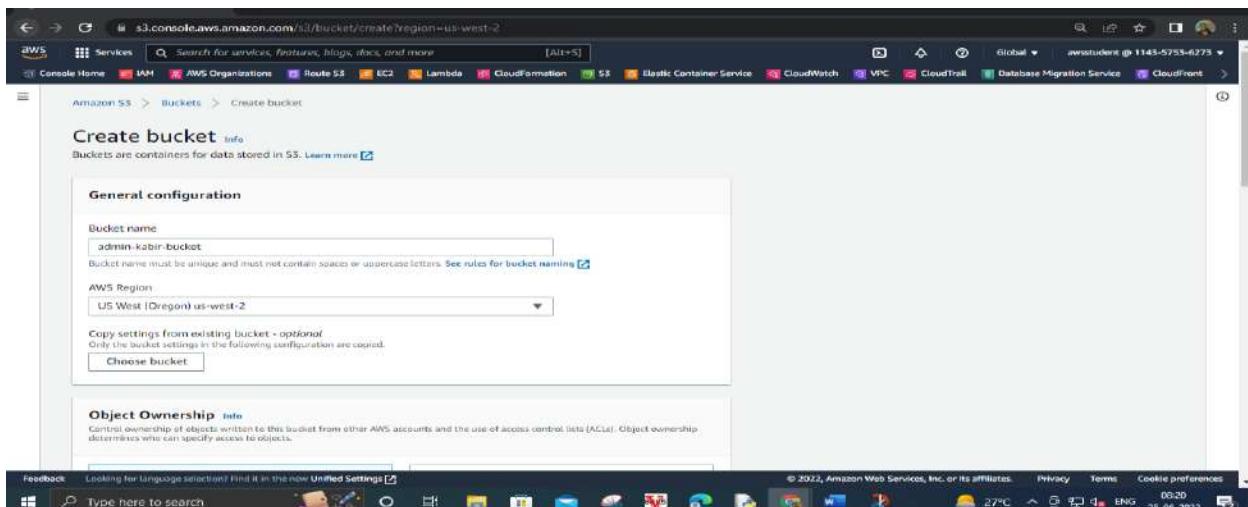
Step 3 – Choose create bucket.



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

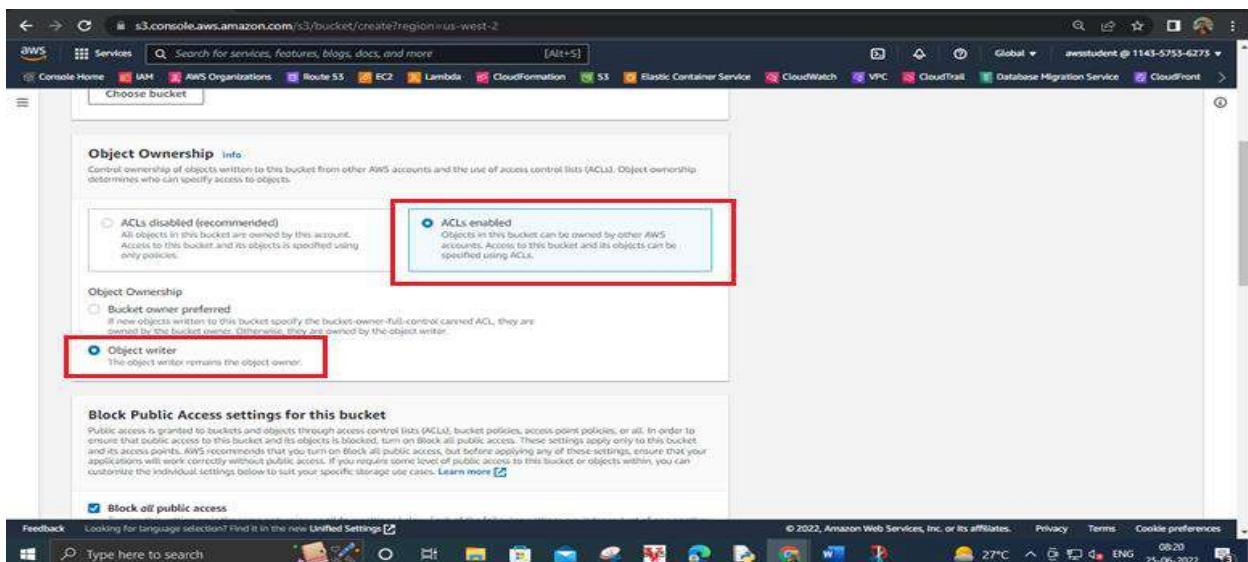
Replace in the bucket name with a random number. This ensures that you have a unique name.

* Example Bucket Name - admin-kabir-bucket987987



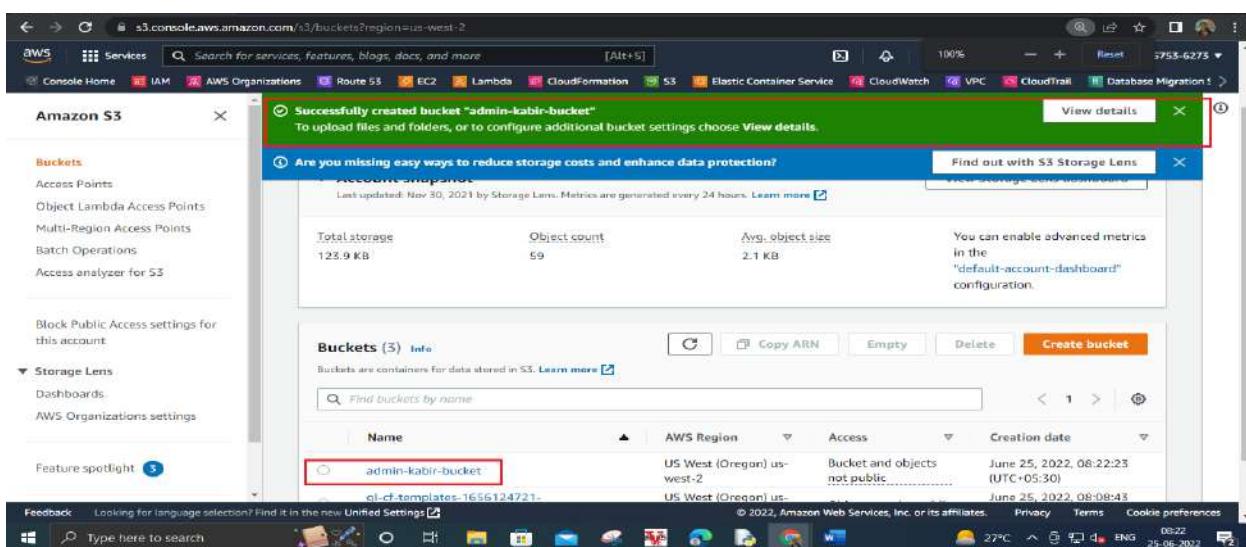
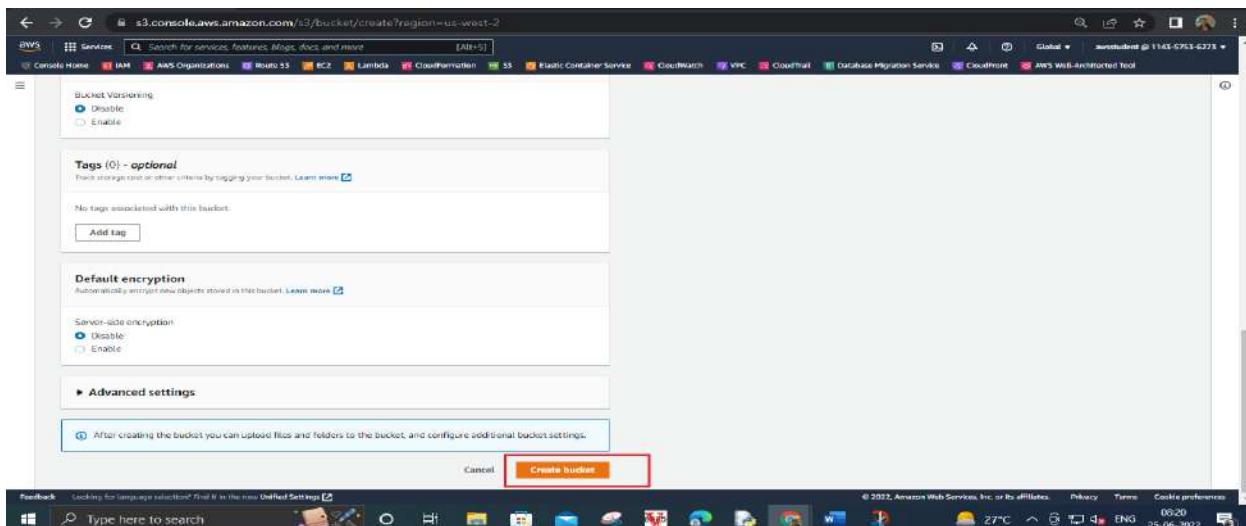
Step 5 – In the Object Ownership section, configure:

- ACLs enabled
- Object Writer



Step 6 – Leave Region as it defaults value.

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

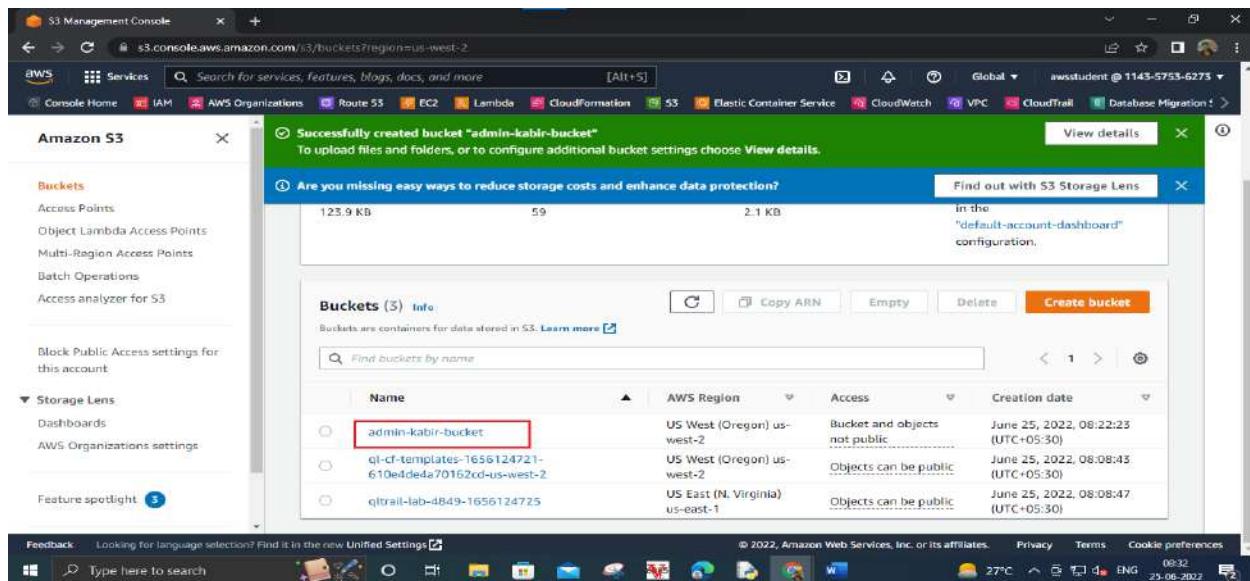


Task 2: Upload an object to the bucket

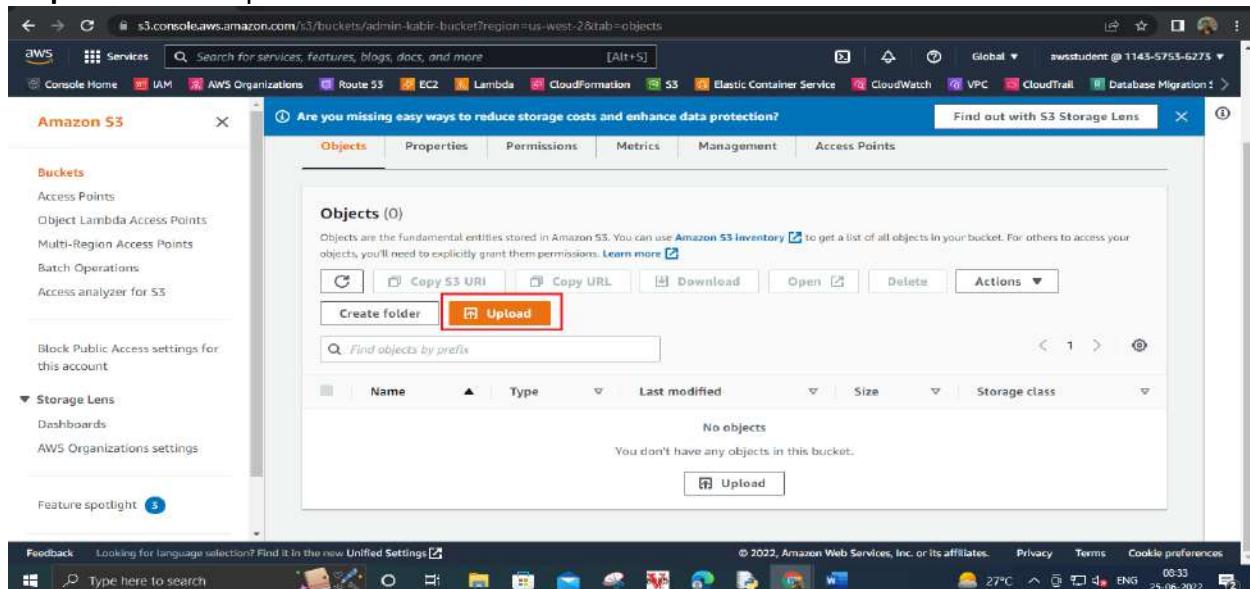
Now that you have a bucket created for your report data, you are ready to work with objects. An object can be any kind of file: a text file, a photo, a video, a zip file, and so on. When you add an object to Amazon S3, you have the option of including metadata with the object and setting permissions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

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

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



Step 9 – Choose Upload.



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

Step 10 – Choose Add files.

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more [?]

Drag and drop files and folders you want to upload here, or choose Add files, or Add folders.

Files and folders (0)

All files and folders in this table will be uploaded.

Add files **Add folder**

Name	Folder	Type	Size
No files or folders			

You have not chosen any files or folders to upload.

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos
- Local Disk (C)
- Local Disk (E)
- Local Disk (F)

Camera Roll Feedback Saved Pictures Screenshots

Capture

File name: [] All Files Open Cancel

No files or folders

You have not chosen any files or folders to upload.

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

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more [?]

Drag and drop files and folders you want to upload here, or choose Add files, or Add folders.

Files and folders (1 Total, 45.5 KB)

All files and folders in this table will be uploaded.

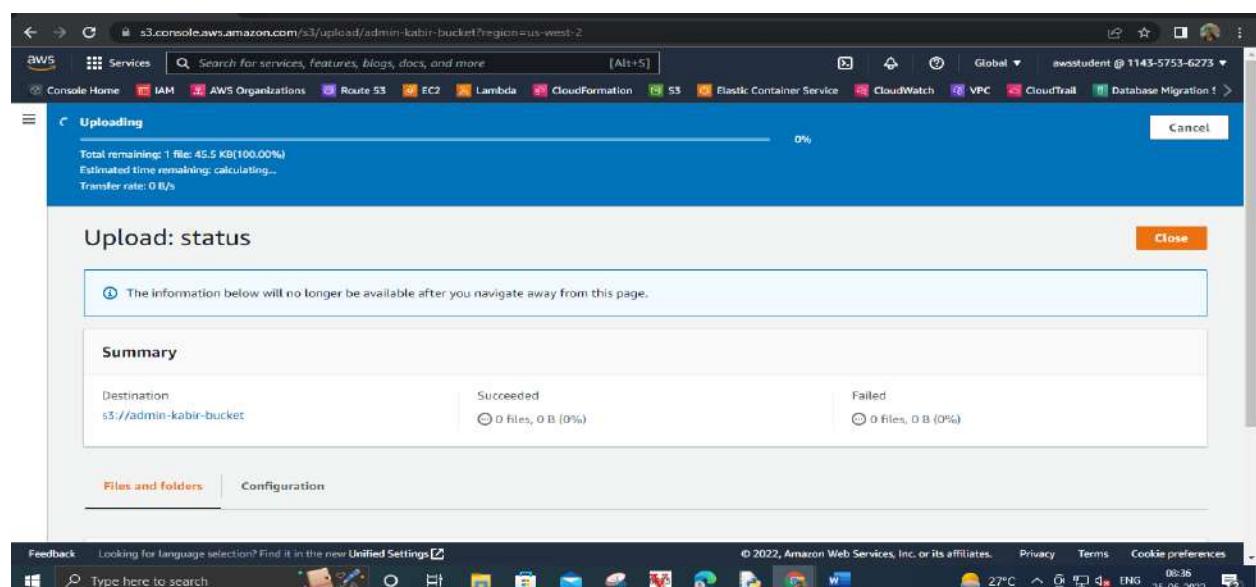
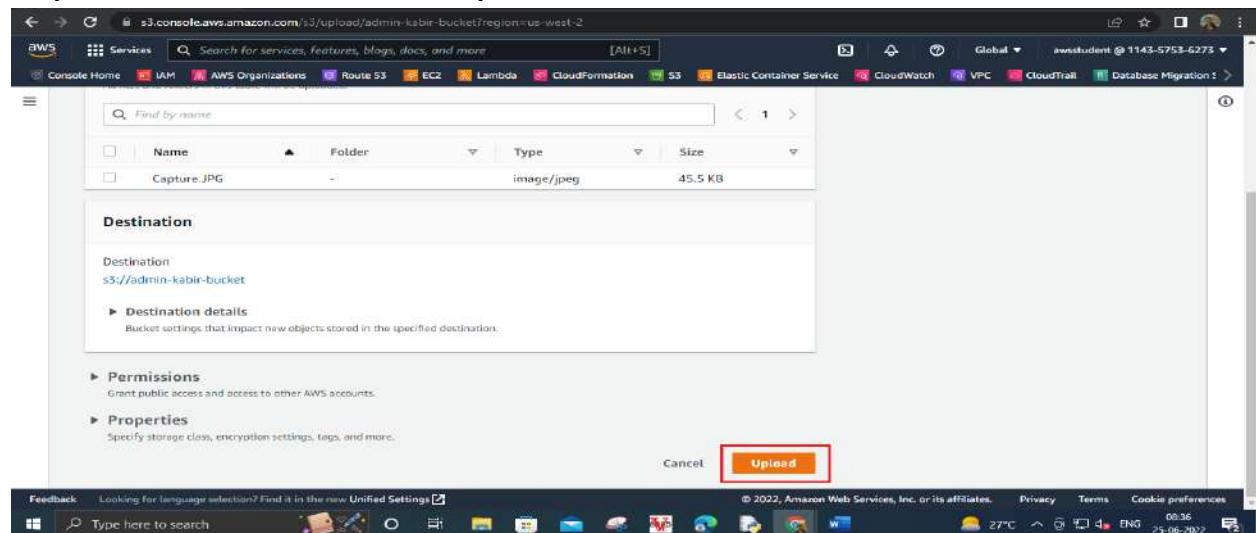
Capture.JPG

Name	Folder	Type	Size
Capture.JPG	-	image/jpeg	45.5 KB

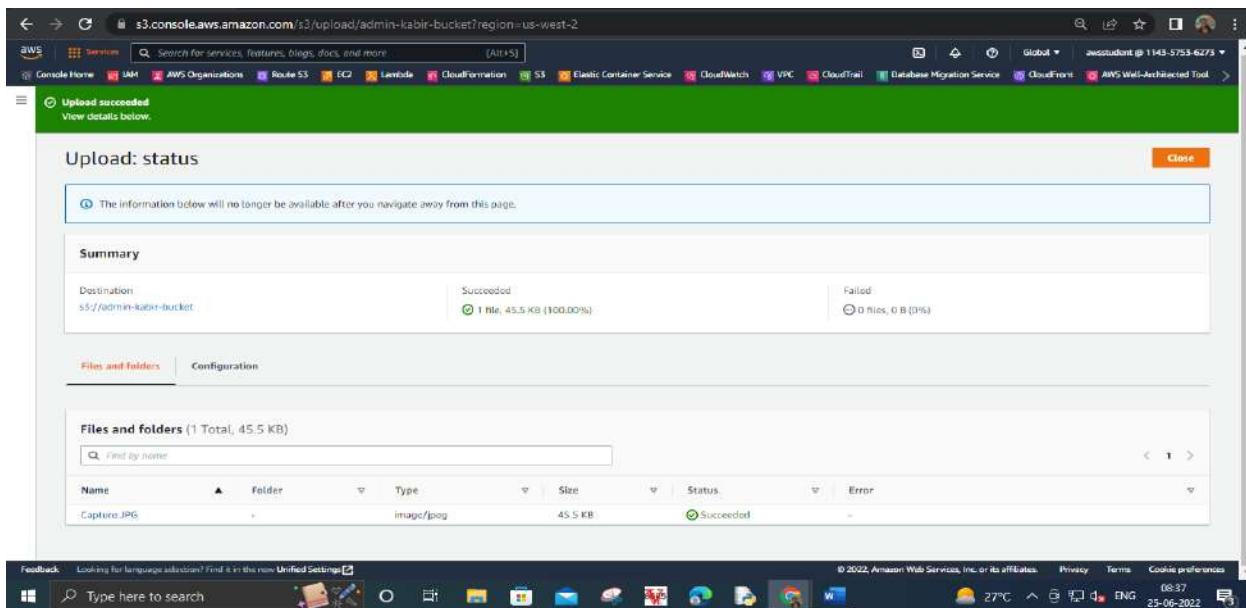
Destination

Destination:

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

Step 11 – Scroll down and choose Upload.

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



In the Upload: status section, choose close.

Task 3: Make an Object public

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

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

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

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

The screenshot shows the AWS S3 console with the URL <https://s3.console.aws.amazon.com/s3/buckets/admin-kabir-bucket?region=us-west-2&tab=objects>. The main content area displays the 'admin-kabir-bucket' overview with the 'Objects' tab selected. It shows one object named 'Capture.JPG' with the following details:

Name	Type	Last modified	Size	Storage class
Capture.JPG	JPG	June 25, 2022, 08:36:38 (UTC+05:30)	45.5 KB	Standard

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

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

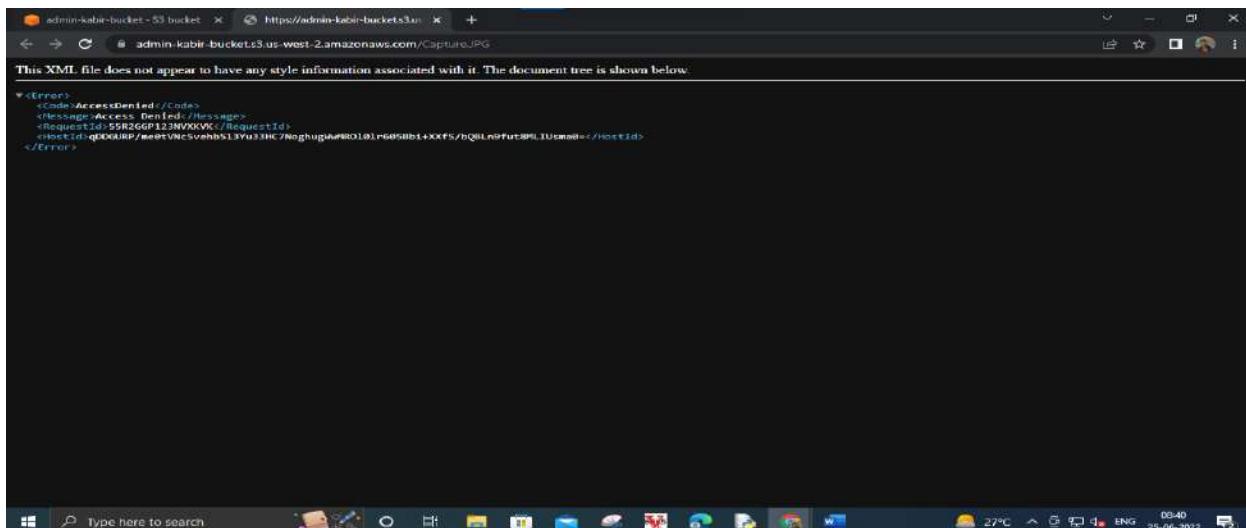
<https://admin-kabir-bucket.s3.us-west-2.amazonaws.com/Capture.JPG>

The screenshot shows the AWS S3 console with the URL <https://s3.console.aws.amazon.com/s3/object/admin-kabir-bucket?region=us-west-2&prefix=Capture.JPG>. The main content area displays the properties for the 'Capture.JPG' object. The 'Properties' tab is selected. The 'Object URL' field is highlighted with a red box and contains the value:

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

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

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



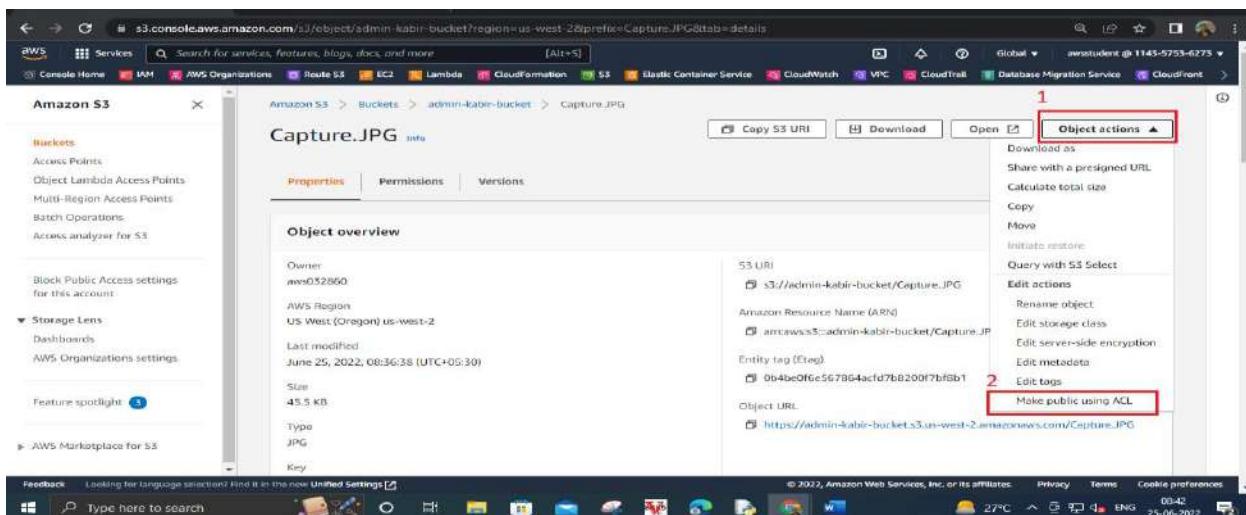
Now that you've confirmed the default security of S3 is private, you want to test how to make the object publicly accessible.

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

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

Step 17 – Close the Show Policy window.

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



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

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

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

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

Step 22 – Choose Permission tab.

The screenshot shows the AWS S3 console with the URL <https://s3.console.aws.amazon.com/s3/object/admin-kabir-bucket?region=us-west-2&tab=permissions>. The page displays the Access Control List (ACL) for the file 'Capture.JPG'. The 'Edit' button in the top right corner of the table is highlighted with a red box.

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: b20ab60f7123d55ddfd33ff01e5e1f1a3d7fe0d5750b50e69672207d394151a	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	-	-

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

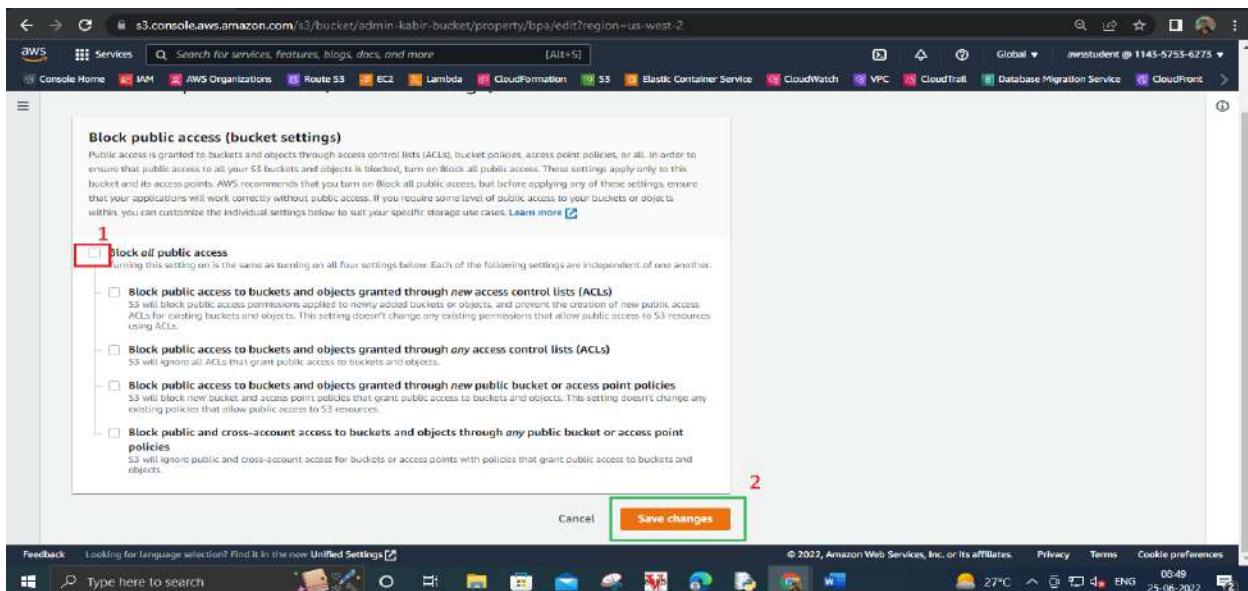
The screenshot shows the AWS S3 console with the URL <https://s3.console.aws.amazon.com/s3/buckets/admin-kabir-bucket?region=us-west-2&tab=permissions>. The page displays the 'Block public access (bucket settings)' section. The 'Edit' button in the top right corner of the table is highlighted with a red box.

Access
Bucket and objects not public

Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLS), bucket policies, access point policies, or all, in order to ensure that public access to all your S3 buckets and objects is blocked, turn on block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

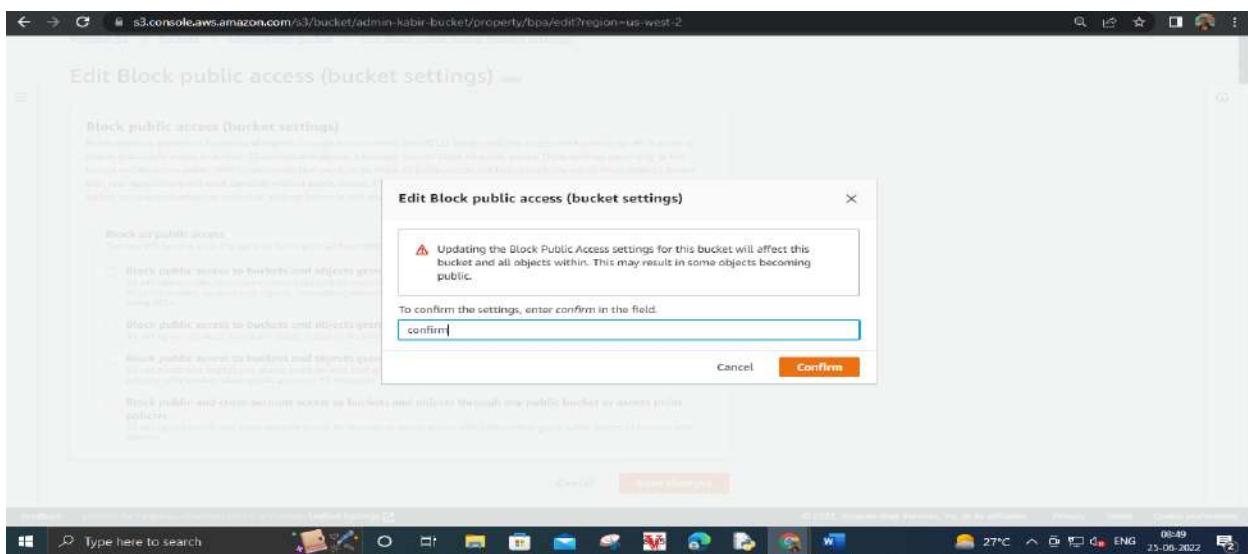
On
Individual Block Public Access settings for this bucket

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



Step 24 – Choose Save Changes.

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



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

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Step 26 – Choose the Objects Tab.

Step 27 – Choose the File name.

Name	Type	Last modified	Size	Storage class
Capture.JPG	JPG	June 25, 2022, 08:36:38 (UTC+05:30)	45.5 KB	Standard

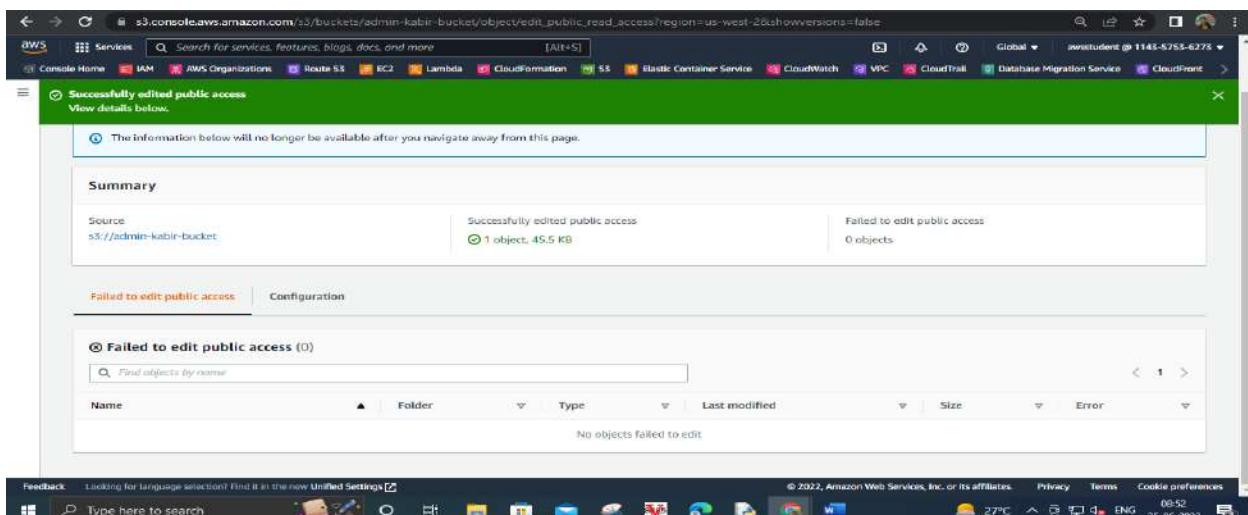
Step 27 – On the Capture.jpg overview page, choose the Object actions button and select Make public via ACL.

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with 'Amazon S3' selected. The main area shows an object named 'Capture.JPG' with its properties: Owner (aws032860), AWS Region (US West (Oregon) us-west-2), Last modified (June 25, 2022, 08:36:38 (UTC+05:30)), Size (45.5 KB), Type (JPG), and Key (Capture.JPG). To the right, the 'Object overview' section displays the object's URI (S3://admin-kabir-bucket/Capture.JPG), ARN (arn:aws:s3:::admin-kabir-bucket/Capture.JPG), Entity tag (Etag) (004be0fe567864acfd7b8200f7bf8b1), Object URL (https://admin-kabir-buckets.s3.us-west-2.amazonaws.com/Capture.JPG), and a 'Make public using ACL' button. A red box highlights the 'Object actions' dropdown menu at the top right, and another red box highlights the 'Make public using ACL' button.

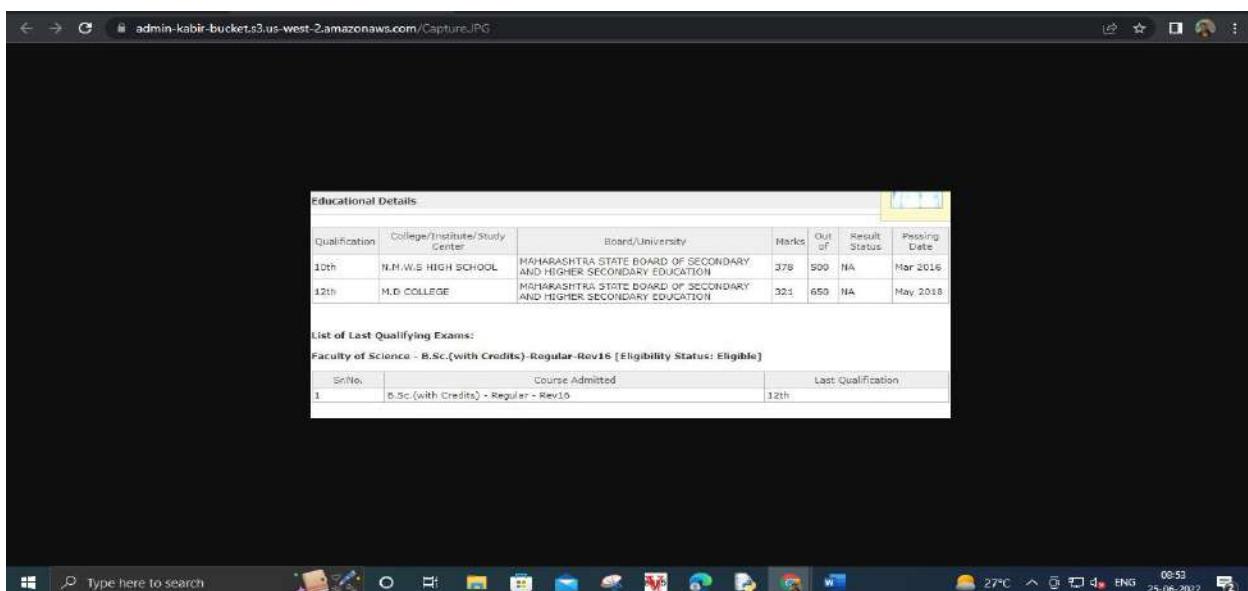
Step 28 – Choose Make public and you should see the green banner Successfully edited public access at the top of the window.

The screenshot shows the 'Make public' dialog box. It contains a warning message: 'When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.' Below this is a table titled 'Specified objects' showing one item: 'Capture.JPG' (Type: JPG, Last modified: June 25, 2022, 08:36:38 (UTC+05:30), Size: 45.5 KB). At the bottom right of the dialog is a 'Make public' button, which is highlighted with a red box. The dialog is centered over the S3 object overview page.

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



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



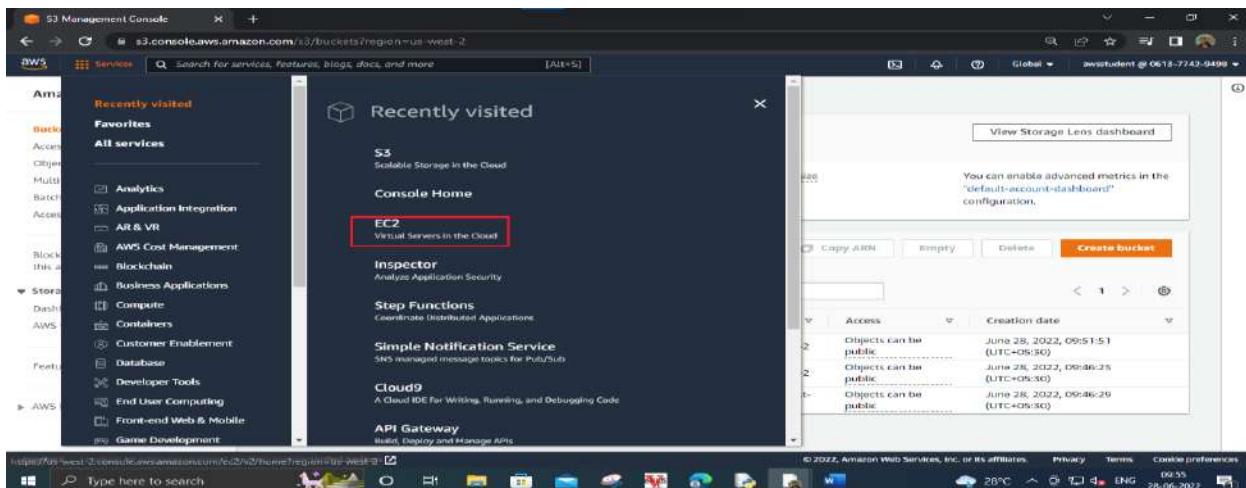
Close the web browser tab that displays your.png image and return to the tab with the Amazon S3 Management Console.

Task 4: Test connectivity from the EC2 instance

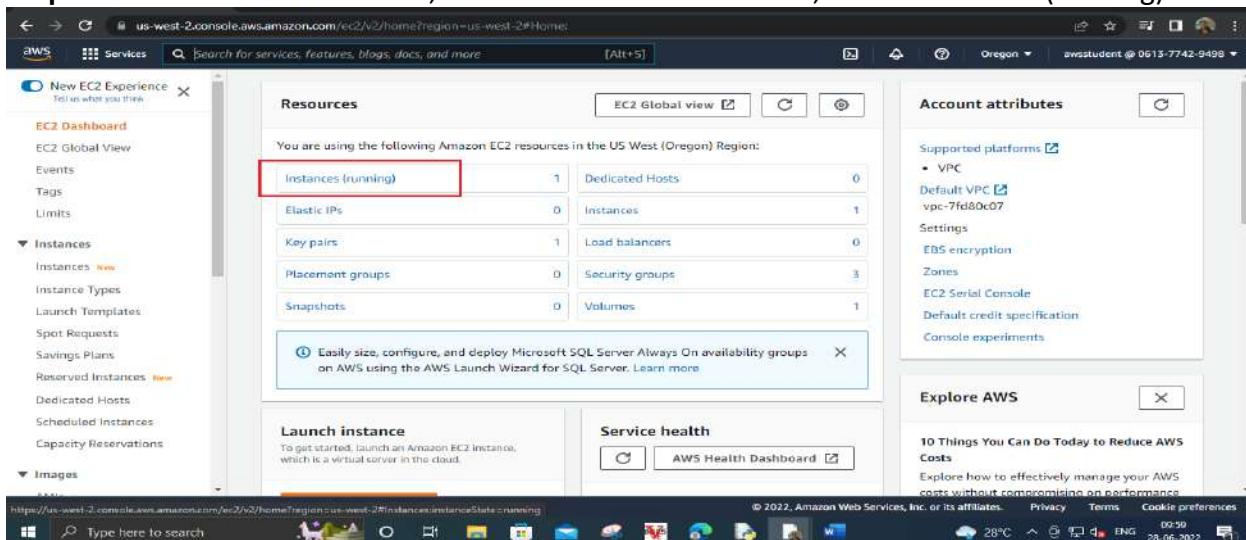
In this task, you connect to your Amazon Elastic Compute Cloud (Amazon EC2) instance to test connectivity and security to the S3 admin-kabir-bucket.

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

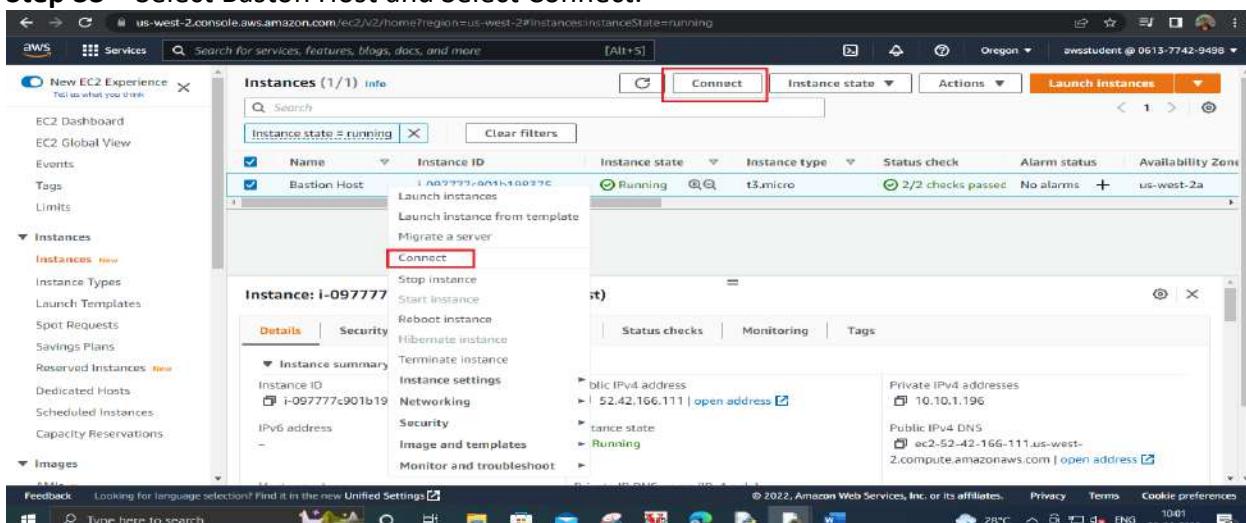
Step 31 – On the service Menu choose EC2.



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

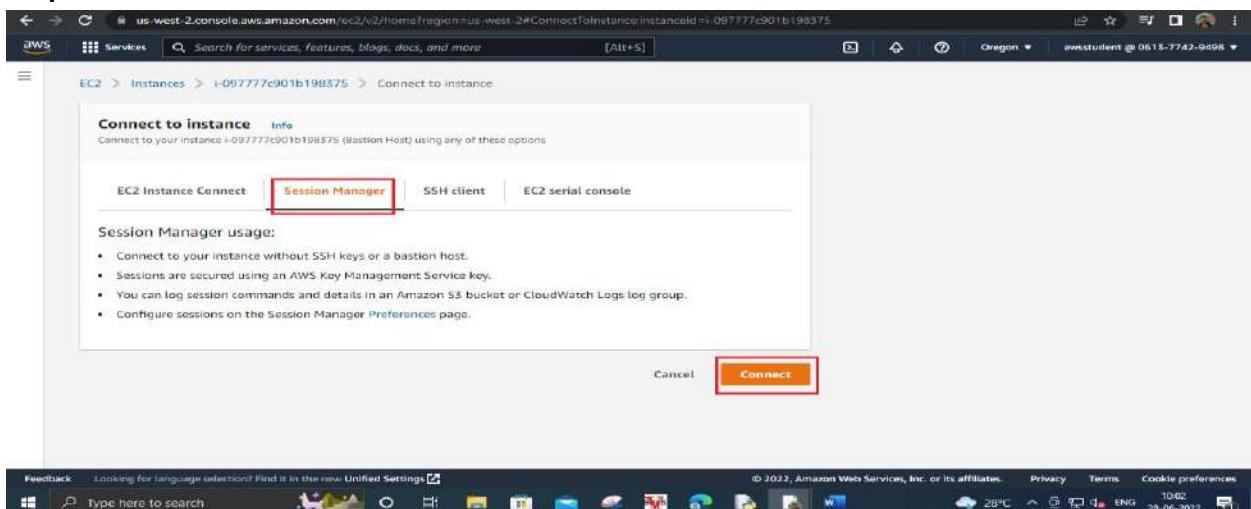


Step 33 – Select Bastion Host and Select Connect.



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

```
cd ~
```



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

```
pwd
```

The output should be:



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

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

```
aws s3 ls
```

The output should look similar to this:

```
Session ID: i-097777c901b198375 Instance ID: i-097777c901b198375# Terminate
sh-4.2$ cd ~
sh-4.2$ pwd
/home/admin-user
sh-4.2$ aws s3 ls
2022-06-28 04:21:51 admin-kabir-bucket
2022-06-28 04:16:25 ql-cf-templates-1656389783-3f97a6cff4a70276-us-west-2
2022-06-28 04:16:29 qltrail-lab-4849-1656389787
sh-4.2$
```

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

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

Step 39 – Enter the following command to list all objects in your admin-kabir-bucket.

Remember to change the number at the end of the admin-kabir-bucket name, to match the name of the bucket you created.

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

The output should look like this:

```
Session ID: i-097777c901b198375 Instance ID: i-097777c901b198375# Terminate
sh-4.2$ cd ~
sh-4.2$ pwd
/home/admin-user
sh-4.2$ aws s3 ls
2022-06-28 04:21:51 admin-kabir-bucket
2022-06-28 04:16:25 ql-cf-templates-1656389783-3f97a6cff4a70276-us-west-2
2022-06-28 04:16:29 qltrail-lab-4849-1656389787
sh-4.2$ aws s3 ls s3://admin-kabir-bucket
2022-06-28 04:22:13        46576 Capture.JPG
sh-4.2$
```

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

```
cd reports
```

```
Session ID: i-097777c901b198375 Instance ID: i-097777c901b198375# Terminate
sh-4.2$ cd ~
sh-4.2$ pwd
/home/admin-user
sh-4.2$ aws s3 ls
2022-06-28 04:21:51 admin-kabir-bucket
2022-06-28 04:16:25 ql-cf-templates-1656389783-3f97a6cff4a70276-us-west-2
2022-06-28 04:16:29 qltrail-lab-4849-1656389787
sh-4.2$ aws s3 ls s3://admin-kabir-bucket
2022-06-28 04:22:13        46576 Capture.JPG
sh-4.2$ ls
reports
sh-4.2$ cd reports/
sh-4.2$
```

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

ls

```
Session ID: awssstudent-0d67482ebb2b41d7f Instance ID: i-097777c901b198375
sh-4.2$ cd ~
sh-4.2$ pwd
/home/ssm-user
sh-4.2$ aws s3 ls
2022-06-28 04:16:25 admin-kabir-bucket
2022-06-28 04:16:25 ql-cf-templates-1656389783-3f97a6cff4a70276-us-west-2
2022-06-28 04:16:29 qltrail-lab-4849-1656389787
sh-4.2$ aws s3 ls s3://admin-kabir-bucket
2022-06-28 04:22:13        46576 Capture.JPG
sh-4.2$ ls
reports
sh-4.2$ cd reports/
sh-4.2$ ls
dolphins.jpg  filen.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.

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

```
Session ID: awssstudent-0d67482ebb2b41d7f Instance ID: i-097777c901b198375
sh-4.2$ cd ~
sh-4.2$ pwd
/home/ssm-user
sh-4.2$ aws s3 ls
2022-06-28 04:21:51 admin-kabir-bucket
2022-06-28 04:16:25 ql-cf-templates-1656389783-3f97a6cff4a70276-us-west-2
2022-06-28 04:16:29 qltrail-lab-4849-1656389787
sh-4.2$ aws s3 ls s3://admin-kabir-bucket
2022-06-28 04:22:13        46576 Capture.JPG
sh-4.2$ ls
reports
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$ aws s3 cp report-test1.txt s3://admin-kabir-bucket
upload failed: ./report-test1.txt to s3://admin-kabir-bucket/report-test1.txt An error occurred (AccessDenied) when calling the PutObject operation:
Access Denied
sh-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.

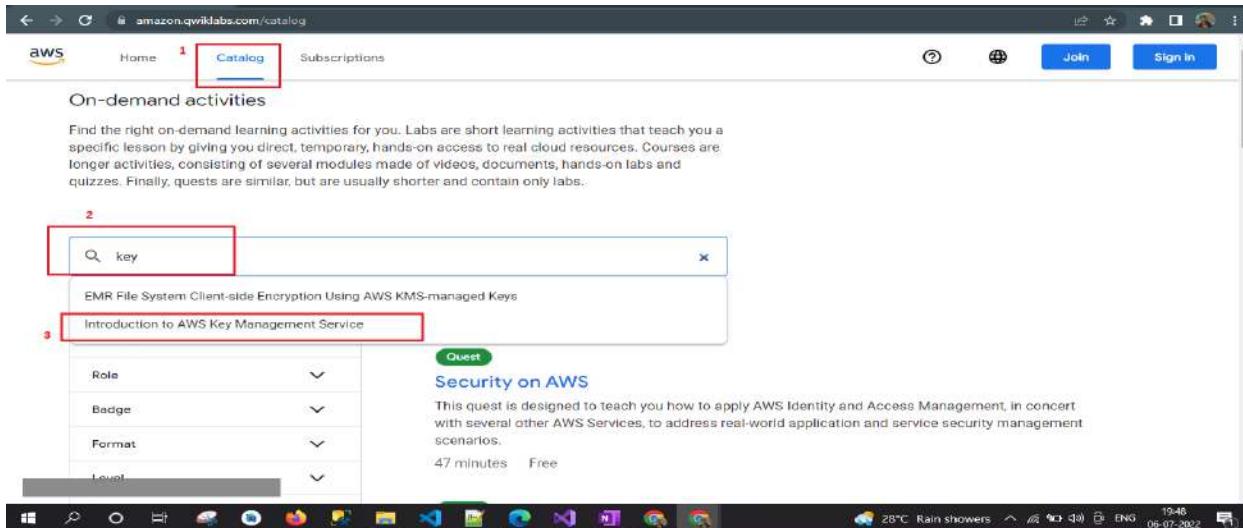
Leave this window open and go back to the AWS Console tab.

Practical 4: Introduction to AWS Key management Service

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

Task 1: Create Your KMS Master Key

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



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

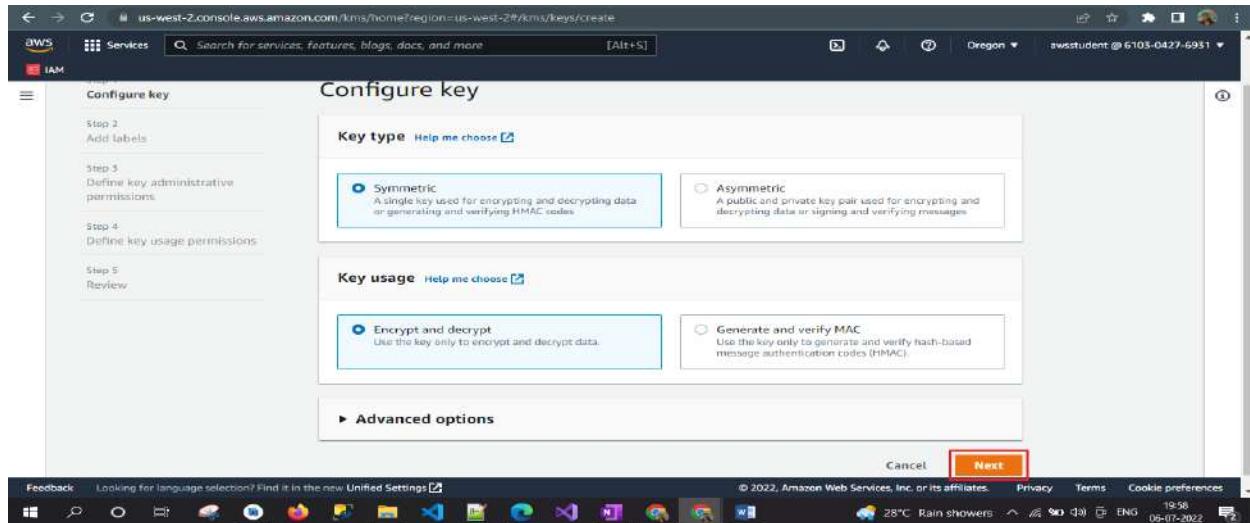


Step 2 – Open your lab by click on the **Open Console** button

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

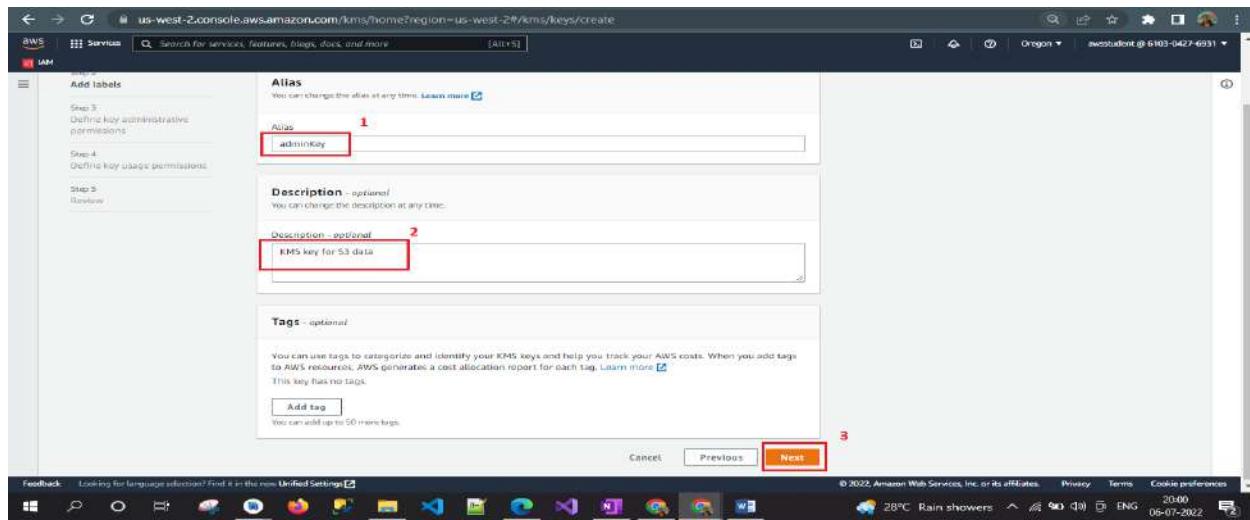
Step 4 – Click Create a key the configure:

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



Step 5 – On the Add Labels page configure:

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



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

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

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

Step 7 – Next.

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

Name	Path	Type
awsstudent	/	User
root-qwkl	/	User
AWSBatchServiceRole	/aws-service-role/awsbatchservice.amazonaws.com/	Role
AWSServiceRoleForAmazonElastiCFileSystem	/aws-service-role/elastifilesystem.amazonaws.com/	Role
AWSServiceRoleForAPIGateway	/aws-service-role/ops.apigateway.amazonaws.com/	Role
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	/aws-service-role/dynamodb.application-autoscaling.amazonaws.com/	Role

Step 9 – Next.

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

cFileSystem	role/elastifilesystem.amazonaws.com/	Role
AWSServiceRoleForAPIGateway	/aws-service-role/ops.apigateway.amazonaws.com/	Role
AWSServiceRoleForApplicationAutoScaling_DynamoDBTable	/aws-service-role/dynamodb.application-autoscaling.amazonaws.com/	Role
AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling.amazonaws.com/	Role
AWSServiceRoleForAWSCloud9	/aws-service-role/cloud9.amazonaws.com/	Role
AWSServiceRoleForAWSLicenseManagerMasterAccountRole	/aws-service-role/license-manager.master-account.amazonaws.com/	Role
AWSServiceRoleForAWSLicenseManagerRole	/aws-service-role/license-manager.amazonaws.com/	Role

Key deletion

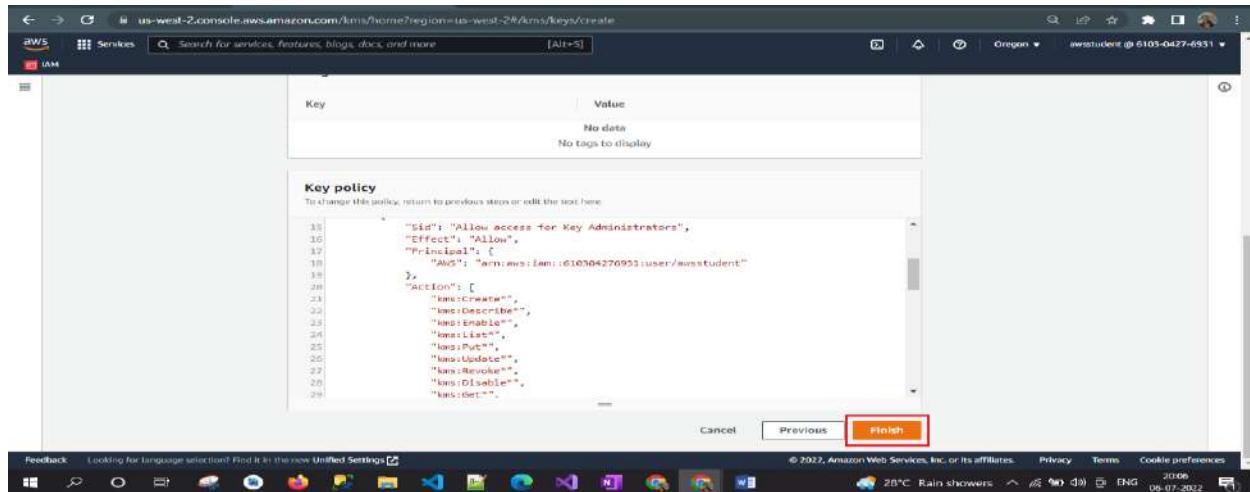
Allow key administrators to delete this key.

Cancel Previous **Next**

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

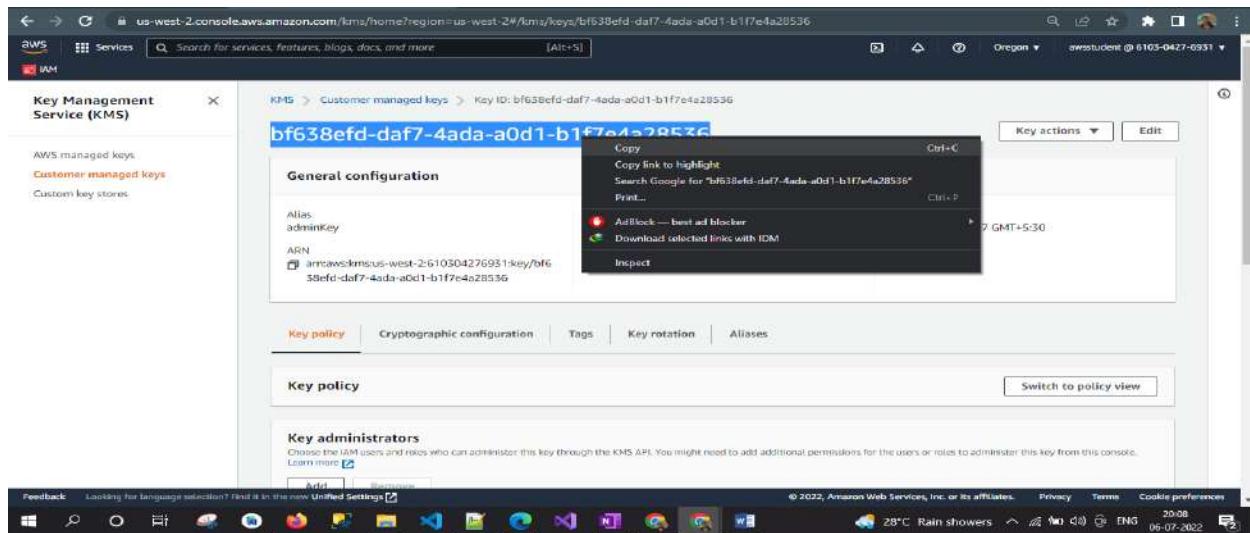
- Review the key policy

- Click Finish.



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

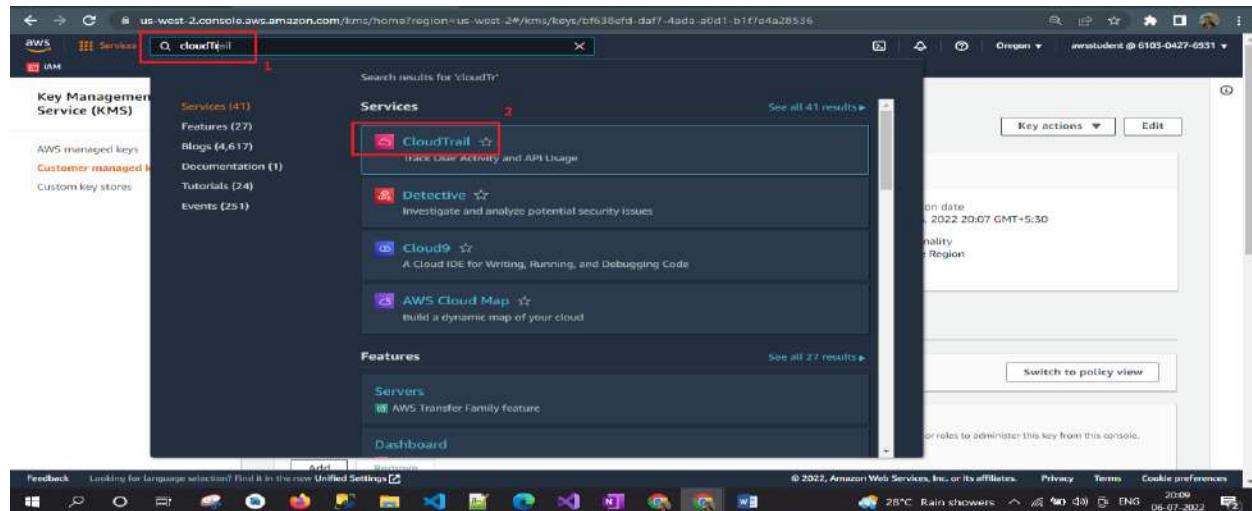
You will use this key id later when looking at the Log activities for this KMS key.



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

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

Step 12 – On the Service menu, click CloudTrail.

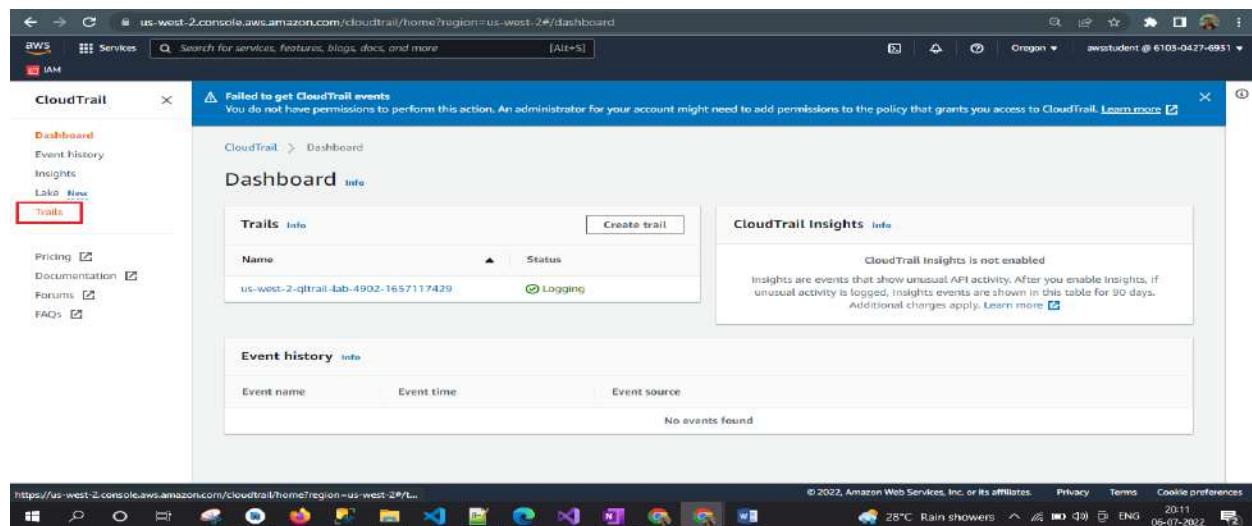


Step 13 – If you see the New Event history features available in the new Cloud trail console with Try Out the new console, click try out the new console, otherwise you can ignore this warning.

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

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

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



Step 17 – Click Create trail then configure:

The screenshot shows the AWS CloudTrail console with the 'Trails' list. A new trail has been created with the name 'us-west-2-cloudtrail-lab-4902-1657117429'. The 'Create trail' button is highlighted with a red box.

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

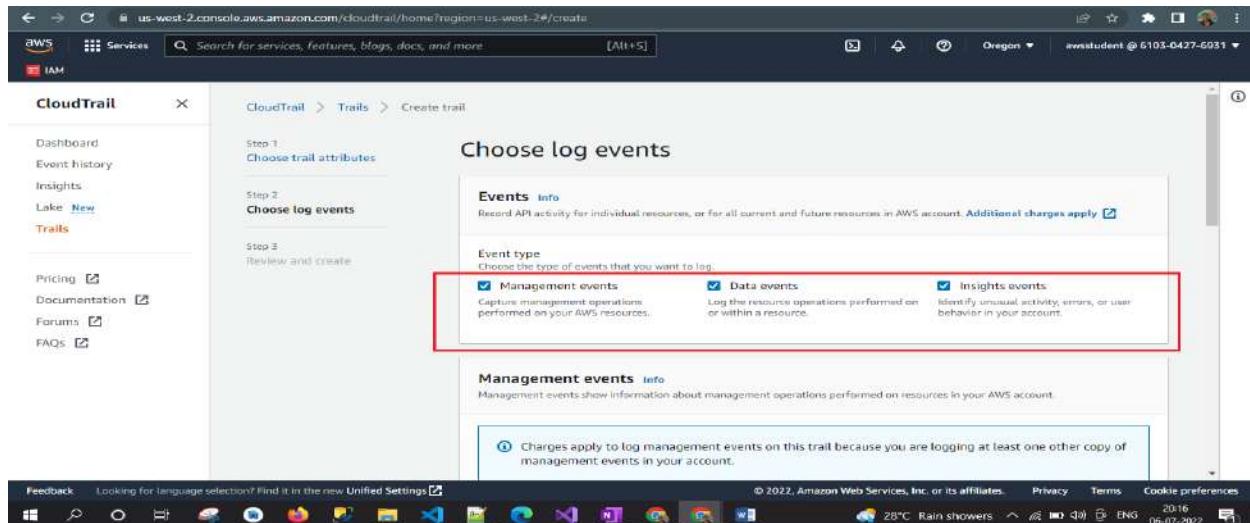
The screenshot shows the 'Choose trail attributes' step in the CloudTrail creation wizard. The 'Trail name' field contains 'adminTrail'. The 'Log file SSE-KMS encryption' checkbox is unchecked. The 'Next Step' button is highlighted with a red box.

Step 18 – Click Next.

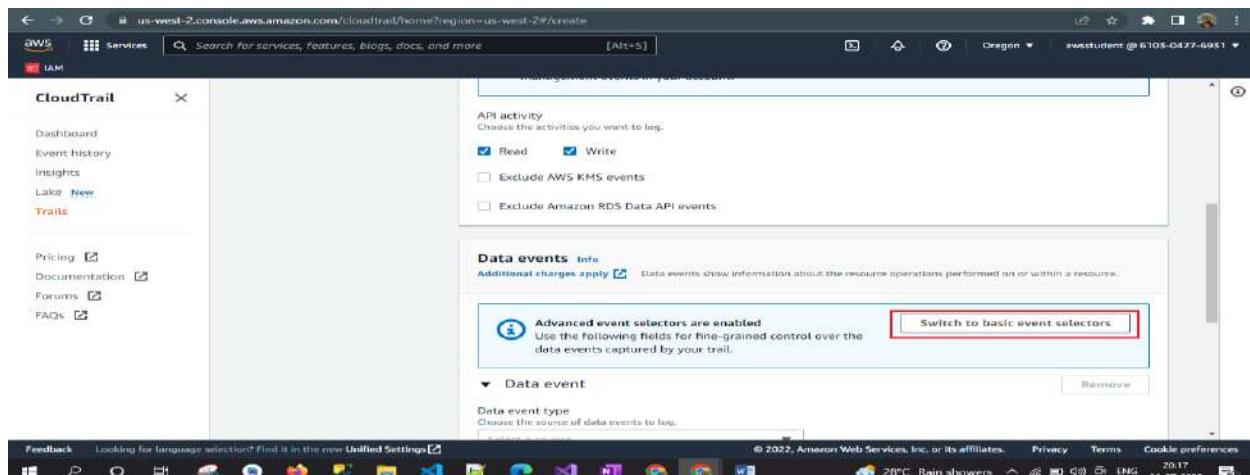
The screenshot shows the 'CloudWatch Logs - optional' step in the CloudTrail creation wizard. The 'Enabled' checkbox is unchecked. The 'Next Step' button is highlighted with a red box.

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

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

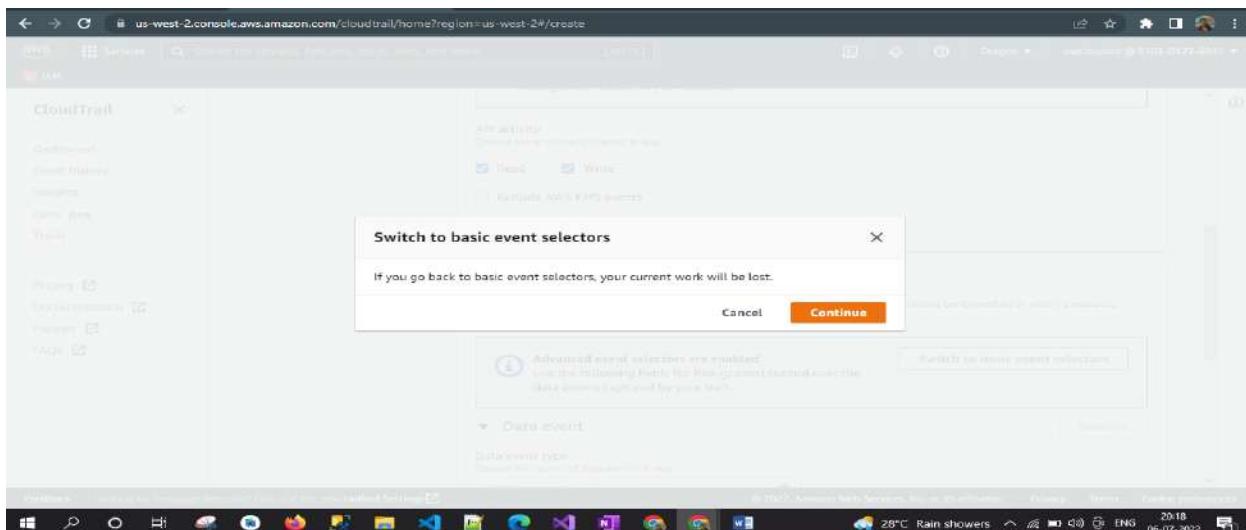


Step 20 – In the Data events, Select Switch to basic event selector.

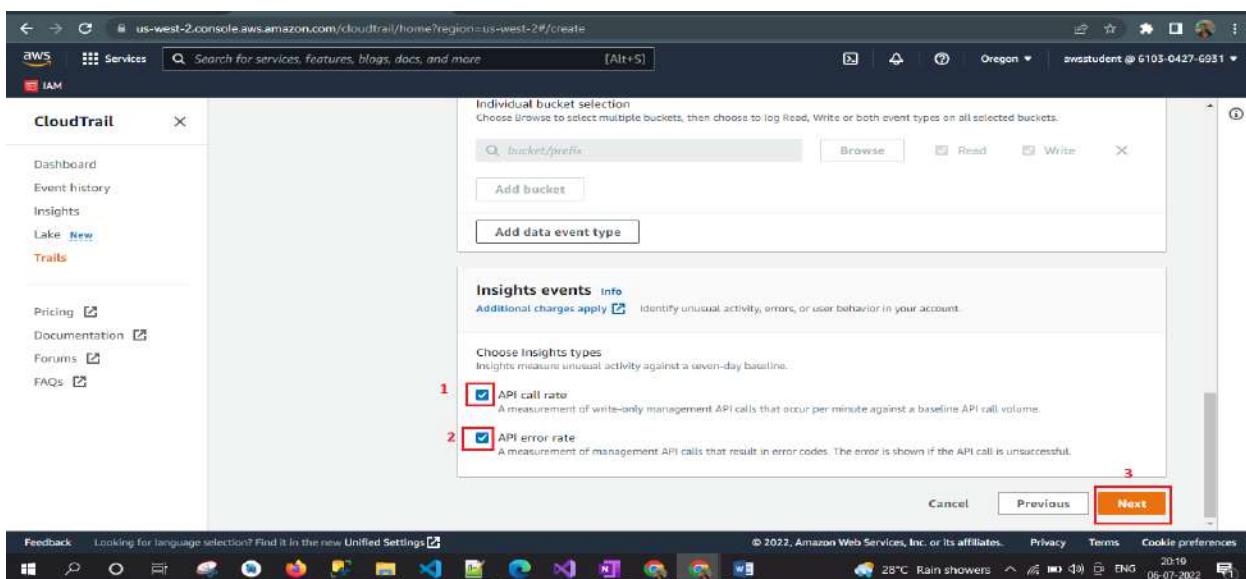


Step 21 – In the Insight event, Select

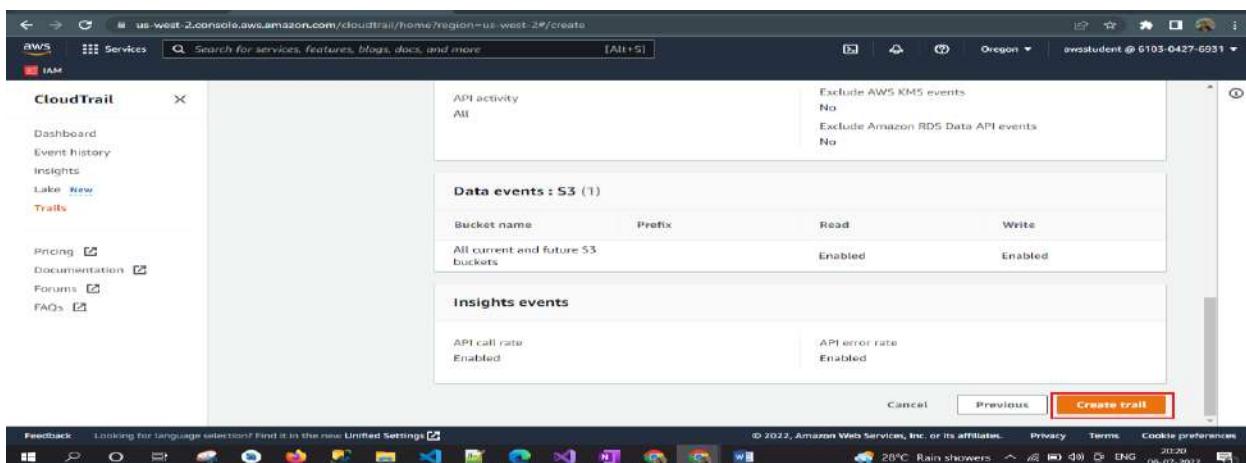
- ✓ API call rate
- ✓ API error rate



Step 22 – Click Next.



Step 23 – Click Create trail.



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

The screenshot shows the AWS CloudTrail Trails page. The left sidebar has links for Dashboard, Event history, Insights, Lake, Trails (which is selected), Pricing, Documentation, Forums, and FAQs. The main content area is titled "Trails" and lists two entries:

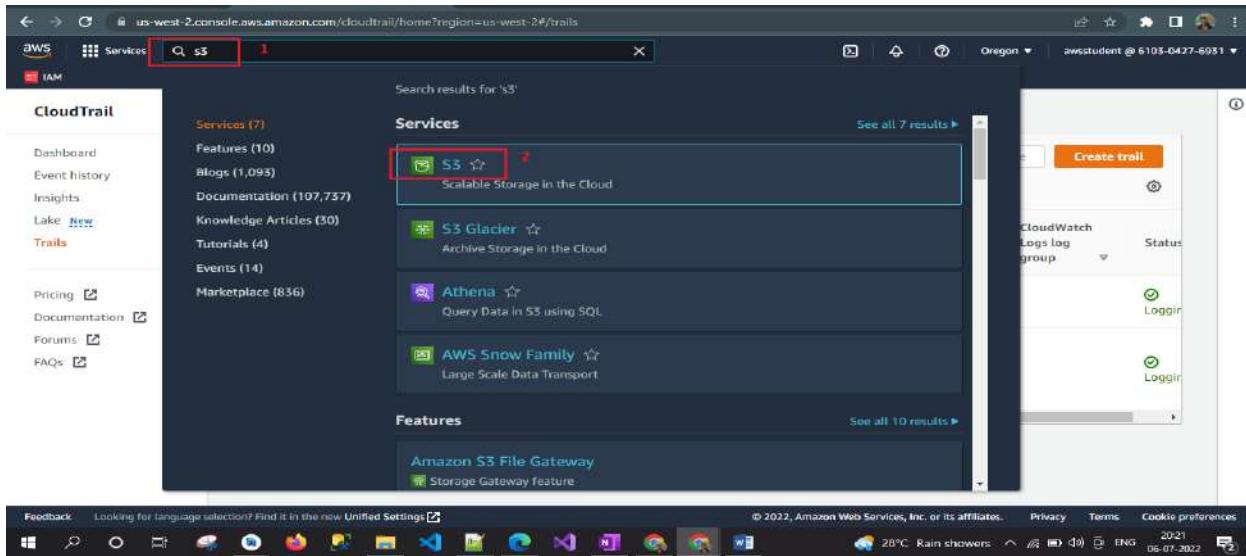
Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
adminTrail	US West (Oregon)	Yes	Enabled	No	admincloudtrailbucket0723	qctrail-lab-4902-1657117429	Logs log group	Logging
us-west-2-qctrail-lab-4902-1657117429	US West (Oregon)	No	Disabled	No				Logging

At the bottom of the page, there are links for Feedback, Unified Settings, Privacy, Terms, and Cookie preferences. The status bar at the bottom right shows the date as 06-07-2022.

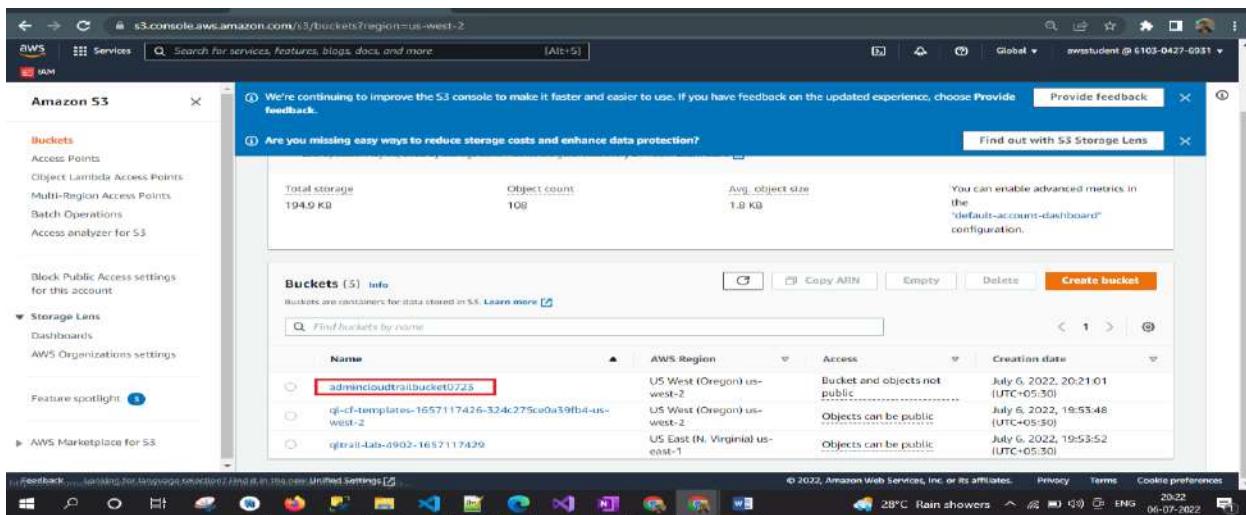
Task 3: Upload an image to your S3 bucket and Encrypt It

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.

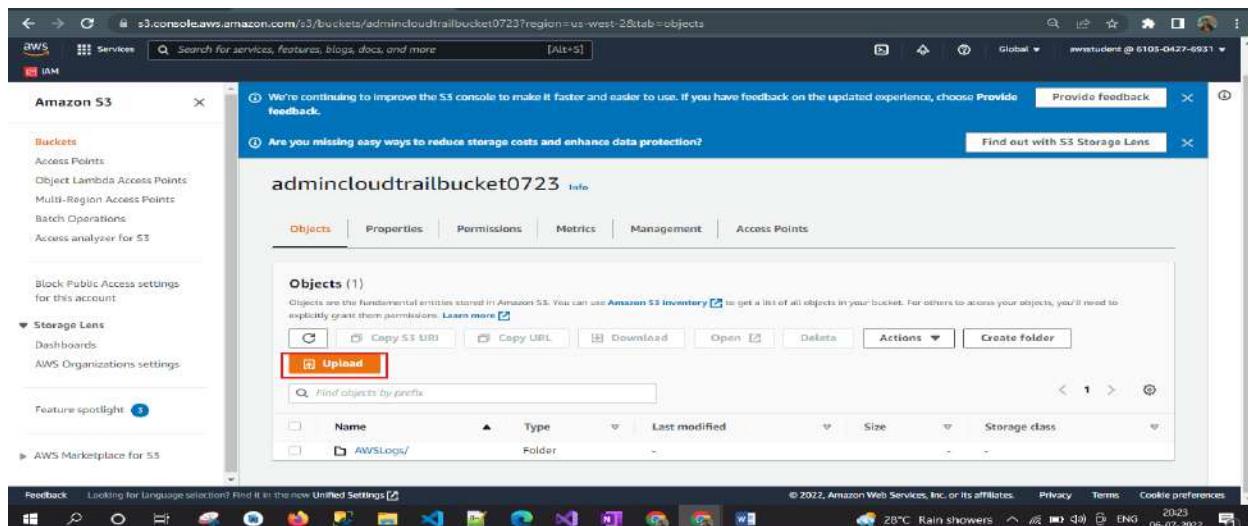
Step 24 – On the Service Menu, click S3.



Step 25 – Click `admincloudtrailbucket0723`.

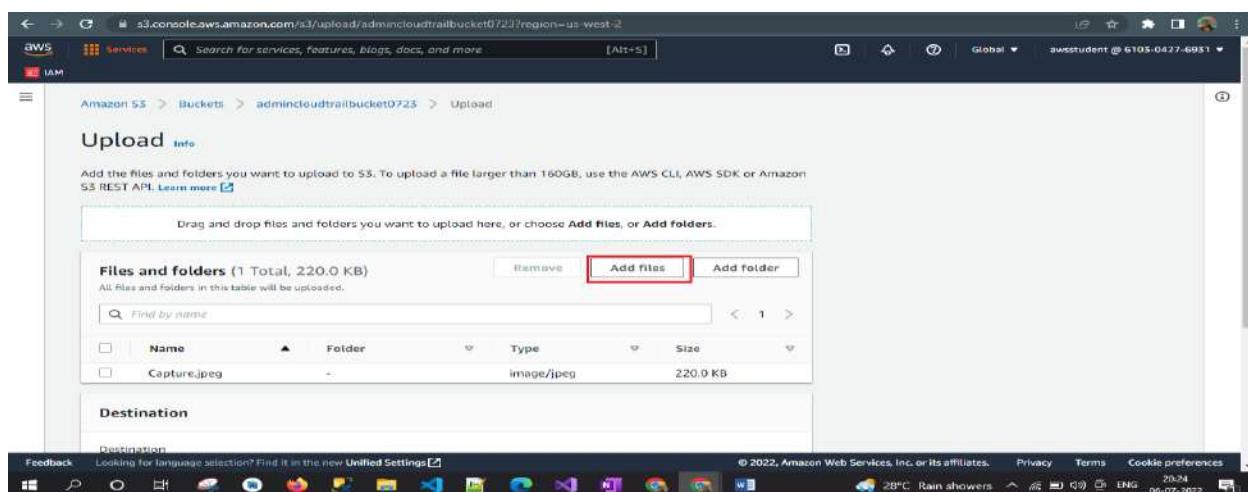


Step 26 – From the objects tab, click **Upload**.



Step 27 – Click Add files.

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



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

The screenshot shows the AWS S3 console with the 'Properties' tab selected under 'Permissions'. The 'Storage class' table lists five options:

Storage class	Designed for	Availability Zones	Min storage duration
<input checked="" type="radio"/> Standard	Frequently accessed data (more than once a month) with milliseconds access	≥ 3	-
<input type="radio"/> Intelligent-Tiering	Data with changing or unknown access patterns	≥ 3	-
<input type="radio"/> Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days
<input type="radio"/> One Zone-IA	Recreatable, infrequently accessed data (once a month) stored in a single zone	1	30 days

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

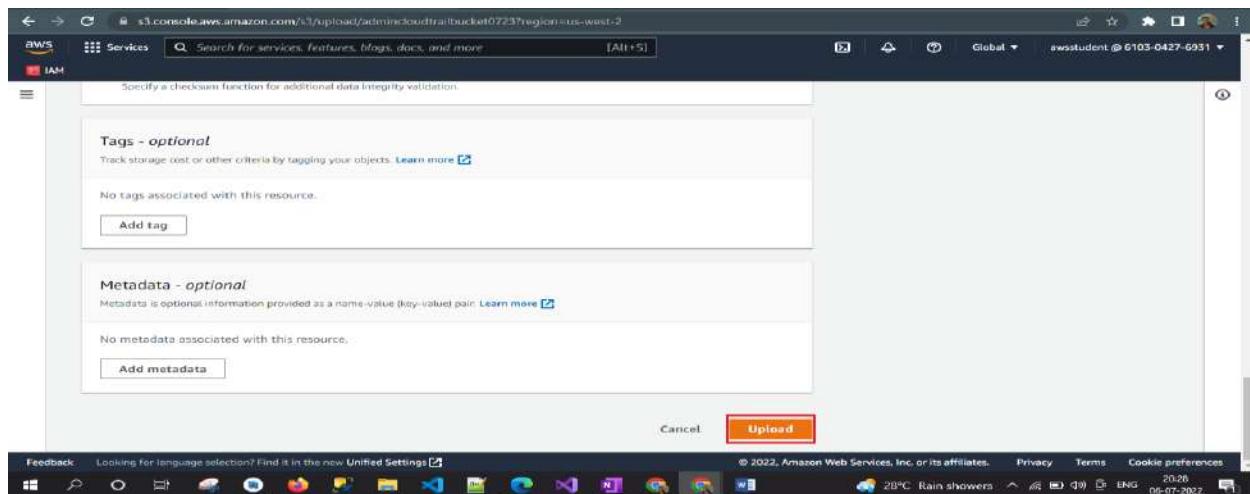
Step 31 – For Encryption Key Type, Select AWS Management Service Key (SSE- KMS).

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

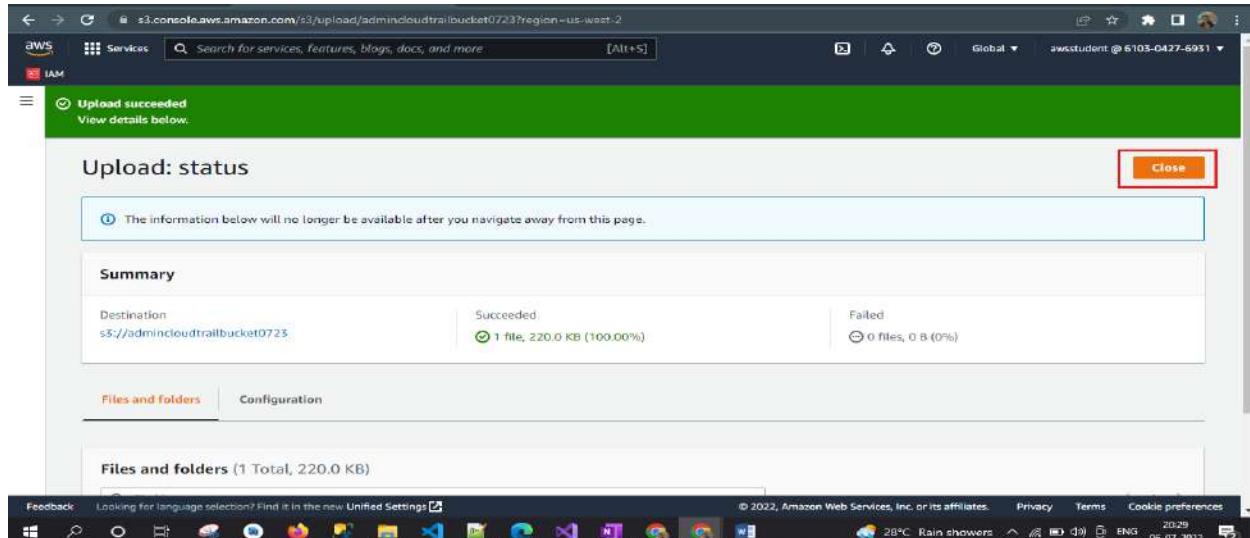
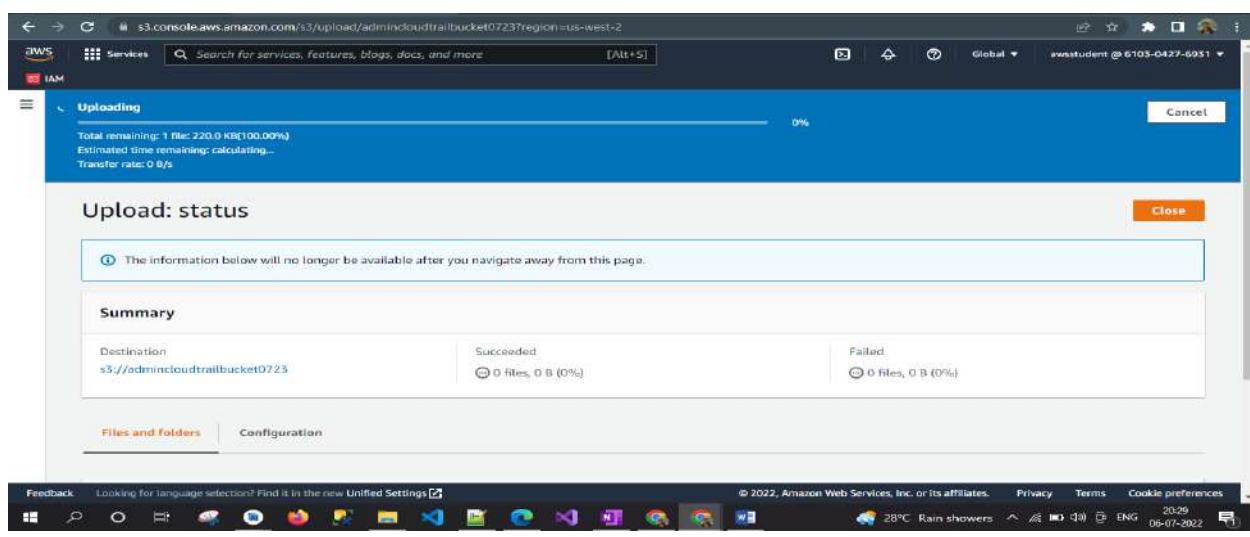
The screenshot shows the 'Server-side encryption settings' section. Under 'Encryption key type', the 'Specify an encryption key' option is selected. Under 'AWS KMS key', the 'Choose from your AWS KMS keys' option is selected. The dropdown menu shows the ARN: arn:aws:kms:us-west-2:610304276951:key/bf638... is highlighted with a red box.

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

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



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



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

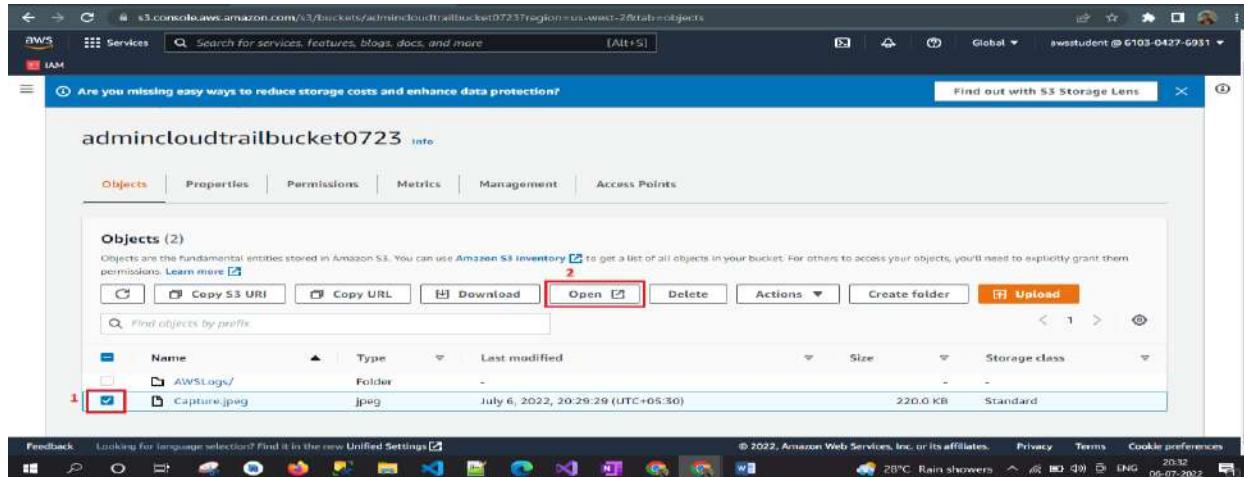
Step 37 – Record the **Last Modified** time to your text editor.

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

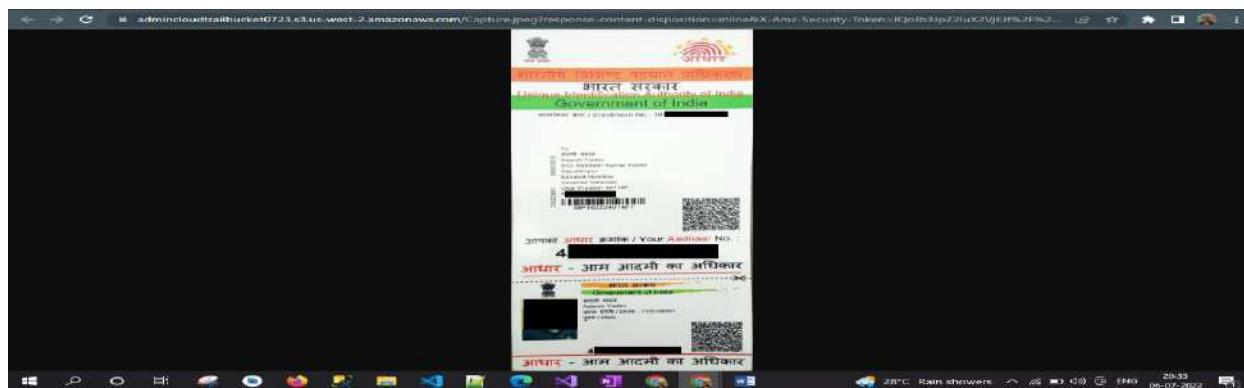
Task 4: Access the Encrypted Image

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

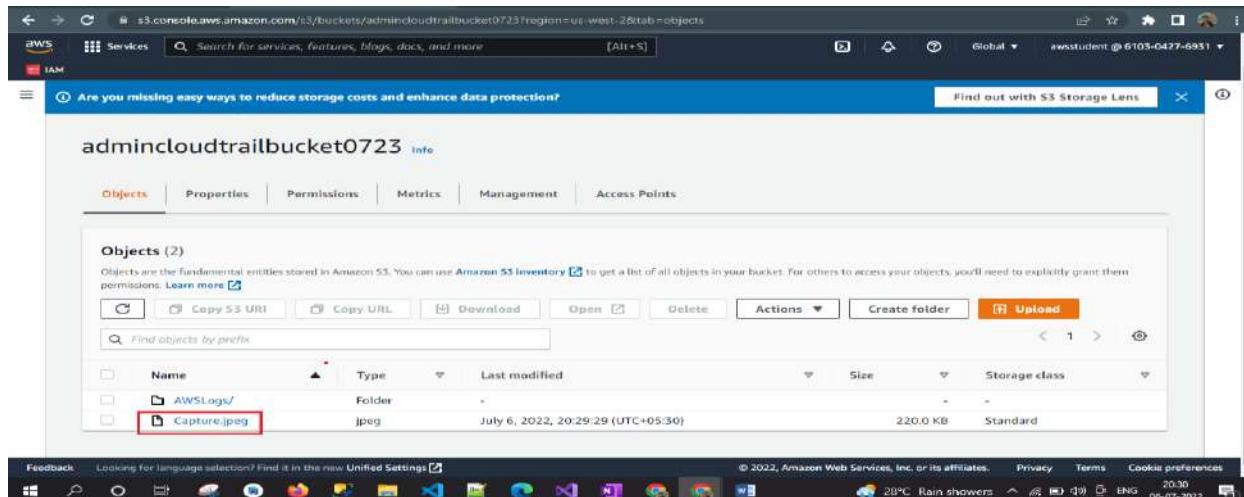
Step 39 – In the Object tab, select image name and then click Open.

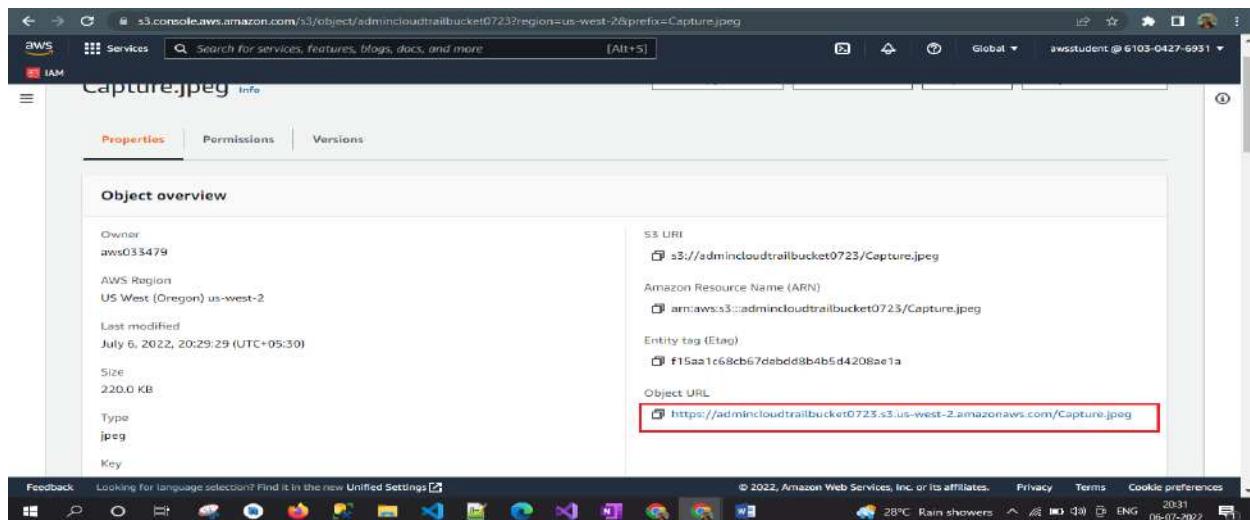


Step 40 – Choose the window/tab that shows your images.



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



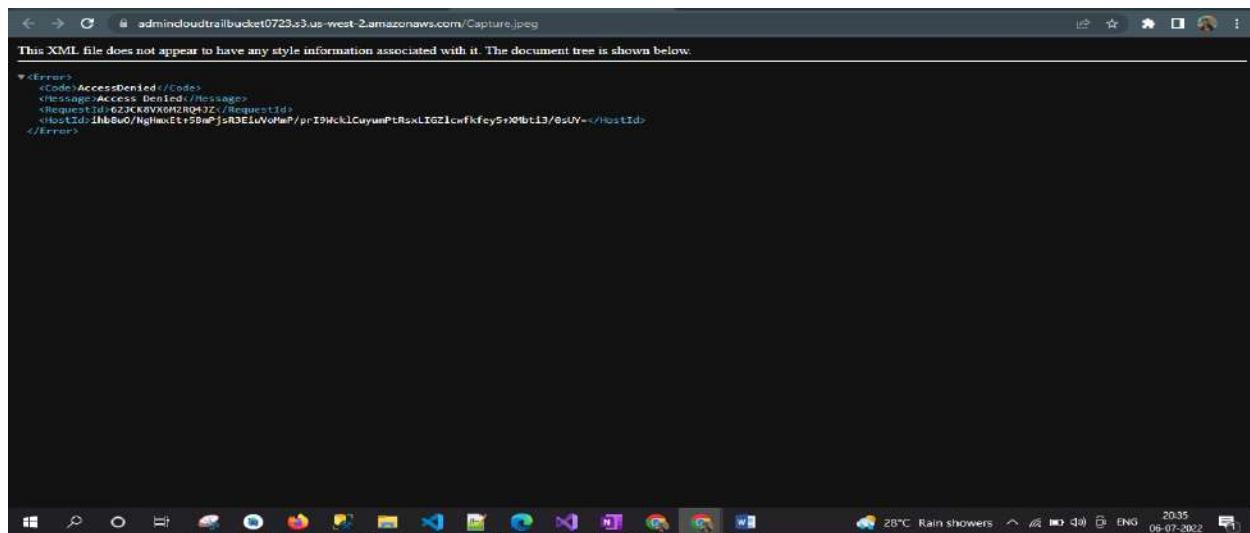


Step 42 – Paste the S3 object URL that you copied earlier into new browser/window.

Step 43 – Press Enter.

Step 44 – What does the page show?

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



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

Step 46 – Click the Permission tab.

Access control list (ACL)

Grant basic read/write permissions to AWS accounts. [Learn more](#)

Grantee	Object	Object ACL
Object owner (your AWS account) Canonical ID: R706f57322078a6f0469a8c9f2ac7b4ab087b78e34cfb97b6cd581bcf0e6c5	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	-	-

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

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

Edit

Block all public access

On

► Individual Block Public Access settings for this bucket

Public access is blocked because Block Public Access settings are turned on for this bucket

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.

Access control list (ACL)

Grant basic read/write permissions to AWS accounts. [Learn more](#)

Grantee	Objects	Object ACL
Object owner (your AWS account)	<input checked="" type="checkbox"/> Read	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write
Everyone (public access) Group: http://acs.amazonaws.com/groups/global/AllUsers	<input type="checkbox"/> Read <input type="checkbox"/> Write	<input type="checkbox"/> Read <input type="checkbox"/> Write

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.

The screenshot shows the AWS S3 console with the URL <https://s3.console.aws.amazon.com/s3/object/admincloudtrailbucket0723?region=us-west-2&prefix=Capture.jpeg>. The 'Object actions' menu is open, and the 'Make public using ACL' option is highlighted with a red box.

Step 52 – Click Make public.

The screenshots show the 'Make public' process:

- The first screenshot shows the 'Specified objects' list with 'Capture.jpeg' selected and the 'Make public' button highlighted.
- The second screenshot shows a green success message: 'Successfully edited public access'.
- The third screenshot shows a summary table with 'Failed to edit public access' status.

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

The screenshot shows the AWS S3 console with the URL <https://s3.console.aws.amazon.com/s3/object/admincloudtrailbucket0723?region=us-west-2&prefix=Capture.jpeg>. The object details are displayed:

- Owner: awso33479
- AWS Region: US West (Oregon) us-west-2
- Last modified: July 6, 2022, 20:29:29 (UTC+05:30)
- Size: 220.0 KB
- Type: jpeg
- Key: Capture.jpeg

On the right, there is a panel with the following fields:

- S3 URI: <https://s3.amazonaws.com/admincloudtrailbucket0723/Capture.jpeg>
- Amazon Resource Name (ARN): <arn:aws:s3:::admincloudtrailbucket0723/Capture.jpeg>
- Entity tag (Etag): <f15aa1c68cb67d8bdd8bdb5d4208ae1a>
- Object URL: <https://admincloudtrailbucket0723.s3.us-west-2.amazonaws.com/Capture.jpeg>

Below the object details, there is an "Object management overview" section and a "Bucket properties" tab. The status bar at the bottom shows the date and time as 06-07-2022, 20:43.

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.

The screenshot shows a browser window with the URL <https://admincloudtrailbucket0723.s3.us-west-2.amazonaws.com/Capture.jpeg>. The page displays an XML error message:

```
<Error>
<Code>InvalidArgument</Code>
<Message>The request specifies Server Side Encryption with AWS KMS managed keys require AWS Signature Version 4.</Message>
<ArgumentName>Authorization</ArgumentName>
<ArgumentValue>AWS4-HMAC-SHA256</ArgumentValue>
<RequestId>D9E1A9A031284025evKwv5/b4ZS3err8DH/sdD7L8dHS/rQa1550haYXynH3Cc=</RequestId>
<HostId>AlloyoMtfC13HAr351284025evKwv5/b4ZS3err8DH/sdD7L8dHS/rQa1550haYXynH3Cc=</HostId>
```

The status bar at the bottom shows the date and time as 06-07-2022, 20:44.

Step 55 – Close the new/tab window.

Task 5: Monitor KMS activity Using CloudTrail Logs.

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

Step 56 – In the AWS management console click Close.

Step 57 – Click the Object tab.

The screenshot shows the AWS S3 console with the path 'Amazon S3 > Buckets > admincloudtrailbucket0723'. The 'Objects' tab is selected. There are two objects listed: 'AWSLogs/' (Type: Folder) and 'Capture.jpeg' (Type: jpg). The 'AWSLogs/' folder is highlighted with a red box. The table headers are 'Name', 'Type', 'Last modified', 'Size', and 'Storage class'. The 'Actions' and 'Upload' buttons are visible at the top of the object list.

The path should look similar to:

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

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

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

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

The screenshot shows the AWS S3 console with the path 'Amazon S3 > Buckets > admincloudtrailbucket0723 > AWSLogs/ > 610304276931/ > CloudTrail/ > us-west-2/ > 2022/ > 07/ > 06/'. The 'Objects' tab is selected. There are 10 objects listed, all ending in '.json.gz'. The 'Actions' and 'Upload' buttons are visible at the top of the object list. The 'Feedback' bar at the bottom indicates 'Looking for language selection? Find it in the new Unified Settings'.

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

Name	Type	Last modified	Size	Storage class
g10304276931_CloudTrail_us-west-2_20220706T1520Z_AbRpTo727QV8Ug0.json.gz	gz	July 6, 2022, 20:47:01 (UTC+05:30)	2.4 kB	Standard
g10304276931_CloudTrail_us-west-2_20220706T1520Z_d4VY4G3sld2AnVi.json.gz	gz	July 6, 2022, 20:46:50 (UTC+05:30)	8.3 kB	Standard
g10304276931_CloudTrail_us-west-2_20220706T15152Z_HW0CJNODErjFfU.json.gz	gz	July 6, 2022, 20:41:51 (UTC+05:30)	10.9 kB	Standard
g10304276931_CloudTrail_us-west-2_20220706T15152Z_CsHPCCLABImve.json.gz	gz	July 6, 2022, 20:41:40 (UTC+05:30)	7.1 kB	Standard
g10304276931_CloudTrail_us-west-2_20220707T1510Z_dyssvD4LDWJaef.json.gz	gz	July 6, 2022, 20:35:29 (UTC+05:30)	7.4 kB	Standard
g10304276931_CloudTrail_us-west-2_20220706T1510Z_dLFWvV5h0kexUj.json.gz	gz	July 6, 2022, 20:36:41 (UTC+05:30)	7.1 kB	Standard
g10304276931_CloudTrail_us-west-2_20220706T1505Z_wBEBXphkmwvWk1Utr.json.gz	gz	July 6, 2022, 20:31:19 (UTC+05:30)	8.6 kB	Standard
g10304276931_CloudTrail_us-west-2_20220706T1505Z_yLFBewOCKoNtB.json.gz	gz	July 6, 2022, 20:31:31 (UTC+05:30)	5.8 kB	Standard
g10304276931_CloudTrail_us-west-2_20220706T1500Z_qJowwvfhSlrgET6.json.gz	gz	July 6, 2022, 20:26:09 (UTC+05:30)	5.2 kB	Standard
g10304276931_CloudTrail_us-west-2_20220706T1500Z_QnqhsVNPrysoEOH.json.gz	gz	July 6, 2022, 20:26:21 (UTC+05:30)	5.8 kB	Standard

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

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

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

Step 61 – Click the latest file in the list.

Step 62 – Click Open.

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

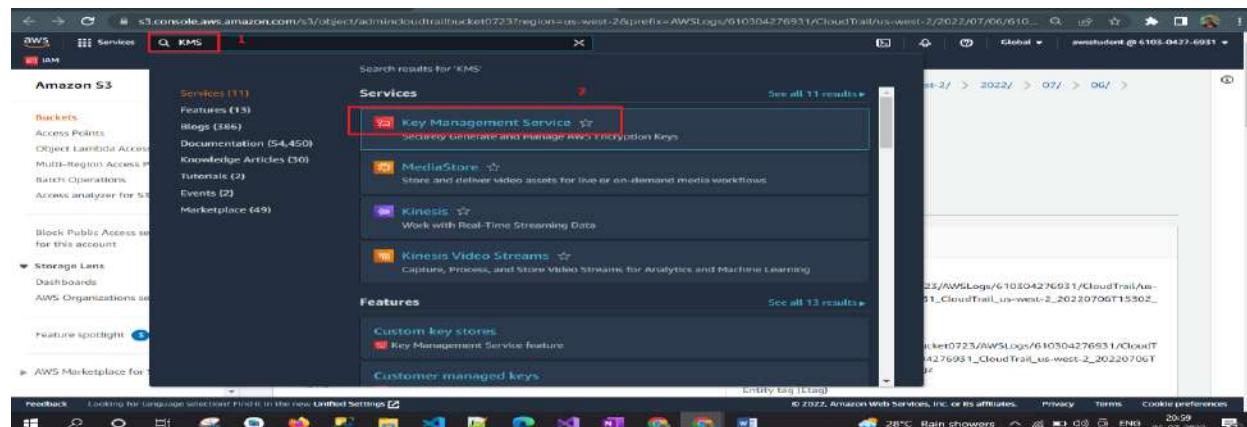
Step 64 – Search for the following in your log file:

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

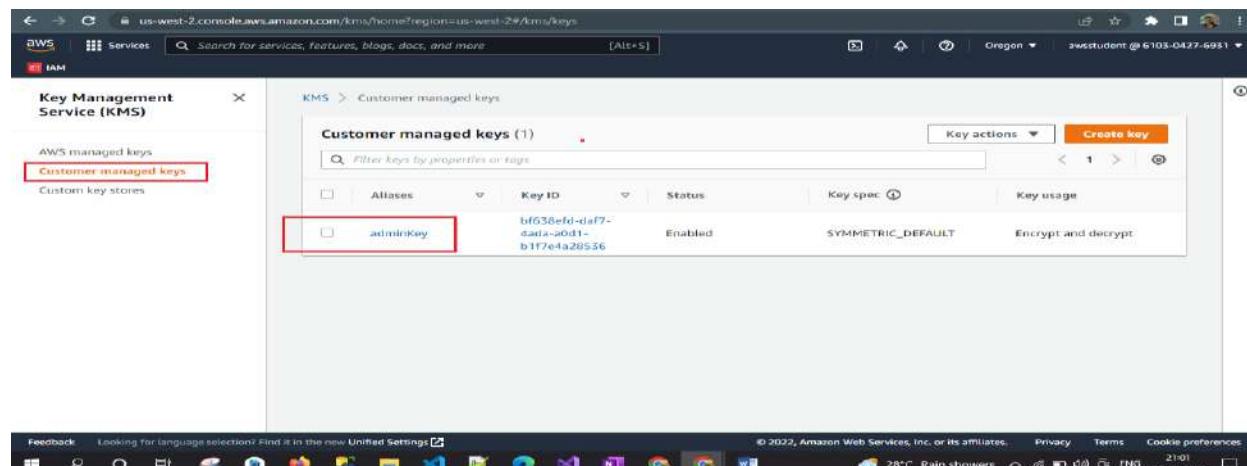
Task 6: Manage Encryption Keys.

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

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



Step 66 – Click adminKey.



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

Step 68 – Click the Remove.

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

The screenshot shows the 'Key deletion' page in the AWS KMS console. Under the 'Key users' section, there is a table with one row. The first column contains a checkbox, which is checked and highlighted with a red box. The second column is 'Name', showing 'awsstudent'. The third column is 'Path', showing '/'. The fourth column is 'Type', showing 'User'. Below the table, there is a 'Remove' button highlighted with a red box.

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 'Key deletion' page in the AWS KMS console. Under the 'Key users' section, the 'Add' button is highlighted with a red box. Below the table, a message says 'Empty Resources' and 'No resources to display'.

The screenshot shows the 'Add key users' dialog box in the AWS KMS console. A table lists IAM users and roles. The first row, 'awsstudent', has a checkbox checked and is highlighted with a red box. The 'Add' button at the bottom right of the dialog is also highlighted with a red box.

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

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

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

Practical 5: Introduction to Amazon DynamoDB

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

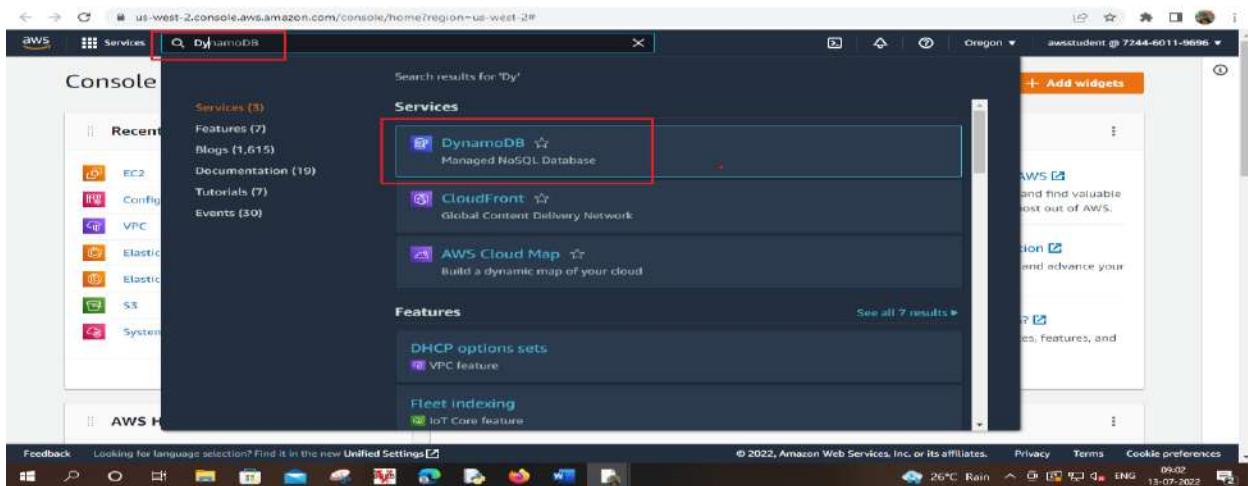
Task 1: Create an Amazon DynamoDB table

Go to the given link

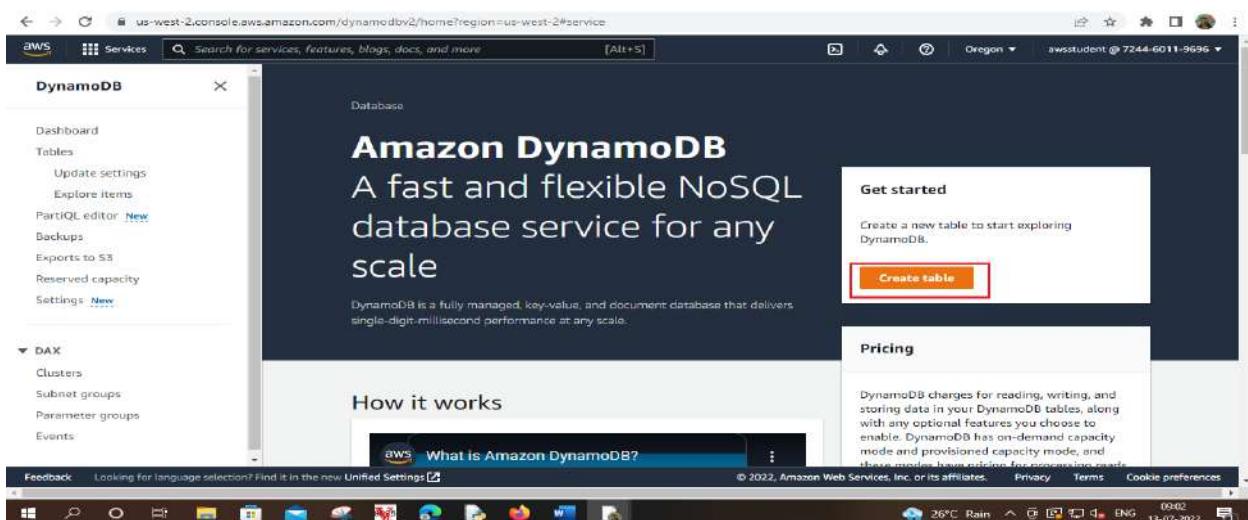
https://amazon.qwiklabs.com/focuses/41738?catalog_rank=%7B%22rank%22%3A46%2C%22num_filter%22%3A1%2C%22has_search%22%3Atrue%7D&parent=catalog&search_id=17288650

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

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



Step 3 – Choose Create table.



Step 4 – For Table name, type: Music

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

Step 6 – For Sort Key, type Song.

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

Table details info

DynamoDB is a schemaless database that requires only a table name and a primary key when you create the table.

Table name
This will be used to identify your table.
Music

Partition key
The partition key is part of the table's primary key. It is a hash value that is used to retrieve items from your table and allocate data across hosts for scalability and availability.
Artist

Sort key - optional
You can use a sort key as the second part of a table's primary key. The sort key allows you to sort or search among all items sharing the same partition key.
Song

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 09:04 13-07-2022

Step 7 – Choose Create table.

The table will be created in less than a minute.

Default settings
The fastest way to create your table. You can modify these settings now or after your table has been created.

Customize settings
Use these advanced features to make DynamoDB work better for your needs.

Default settings
Using default settings configures your table with standard values. Some settings can be changed after table creation.

Tags
Tags are pairs of keys and optional values, that you can assign to AWS resources. You can use tags to control access to your resources or track your AWS spending.

No tags are associated with the resource.
Add new tag
You can add 50 more tags.

This table will be created with auto scaling disabled. You do not have permissions to enable auto scaling.

Cancel **Create table** © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 26°C Rain 09:05 13-07-2022

Step 8 – Wait for your table to be created.

DynamoDB **Creating the Music table. It will be available for use shortly.**

DynamoDB > Tables

Tables (1) info

Na...	Status	Partition key	Sort key	Indexes	Read capacity mode	Write capacity mode
Music	Creating	Artist (\$)	Song (\$)	0	Provisioned (5)	Provisioned (5)

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 09:05 13-07-2022

The screenshot shows the AWS DynamoDB console. On the left, there's a navigation pane with options like Dashboard, Tables (which is selected), Update settings, Explore items, PartiQL editor, Backups, Exports to S3, Reserved capacity, and Settings. Below that is a section for DAX with Clusters, Subnet groups, Parameter groups, and Events. The main area is titled 'Tables (1) Info' and shows a table named 'Music'. The table has one item with the partition key 'Artist (S)' and sort key 'Song (S)'. The item is provisioned with 0 reads and 5 writes. The status is 'Active'. There are buttons for Actions, Delete, and Create table. A search bar at the top says 'Search for services, features, blogs, docs, and more...'. The bottom of the screen shows the Windows taskbar with various icons and the system tray.

Task 2: Add Data

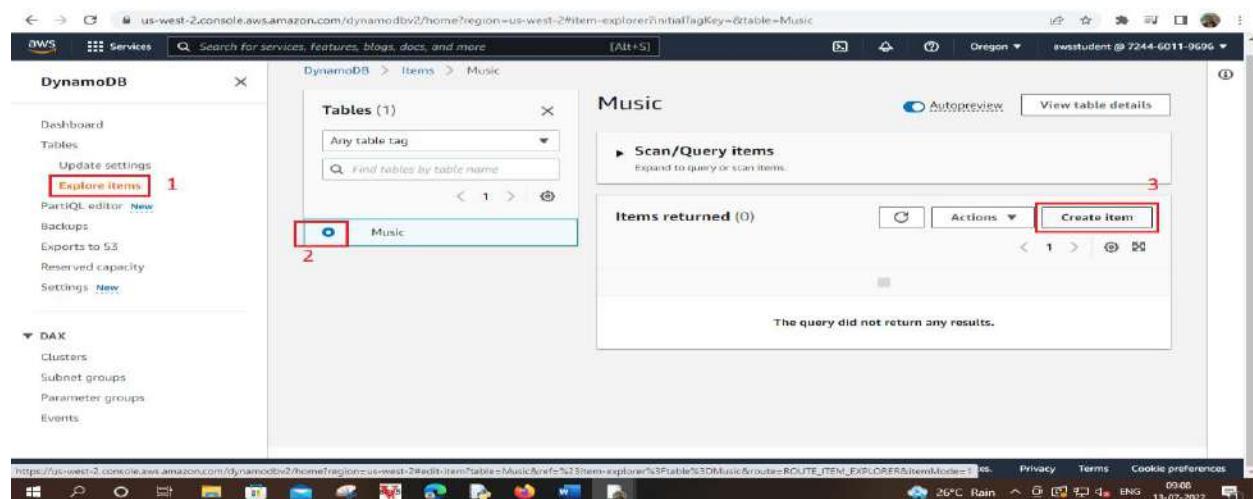
In this task, you will add data to the table. A table is a collection of data on a particular topic.

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

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

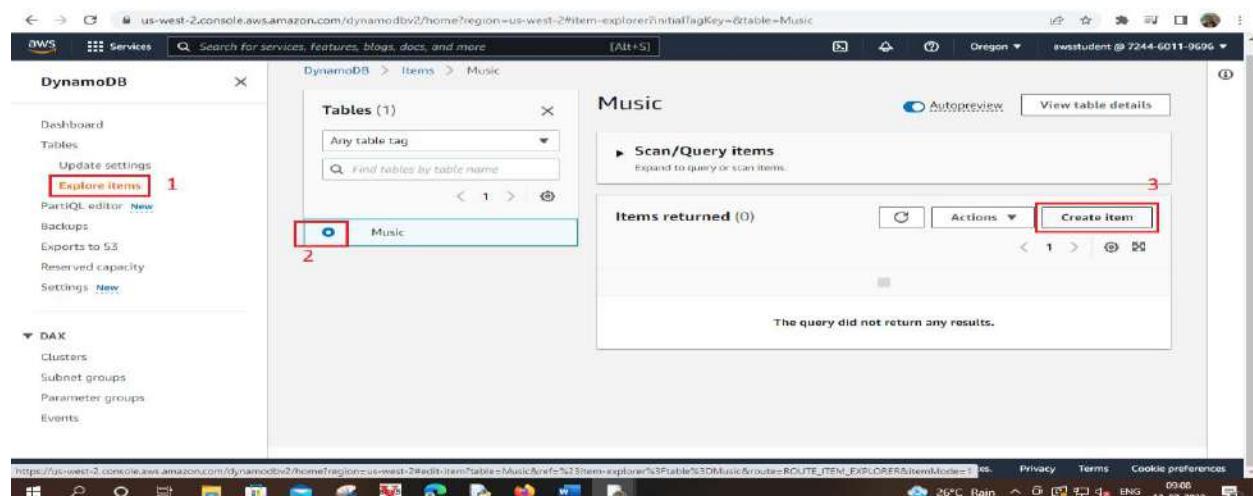
When you write an item to a DynamoDB table, only the Primary Key and Sort Key (if used) are required. Other than these fields, the table does not require a schema. This means that you can add attributes to one item that may be different to the attributes on other items.

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



Step 10 – Select Music.

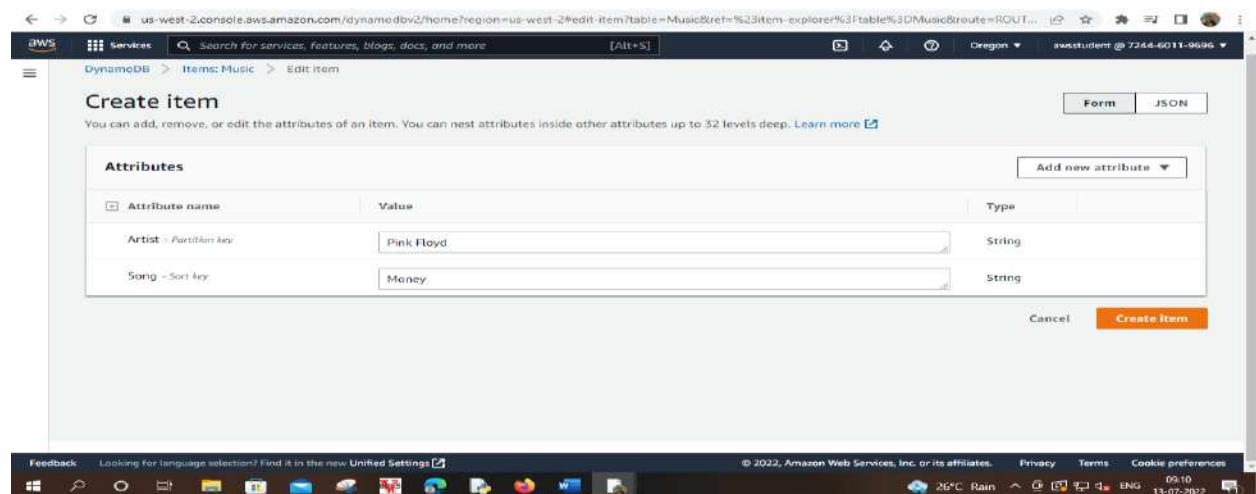
Step 11 – Choose Create Item.



Step 12 – For Artist String, type: Pink Floyd

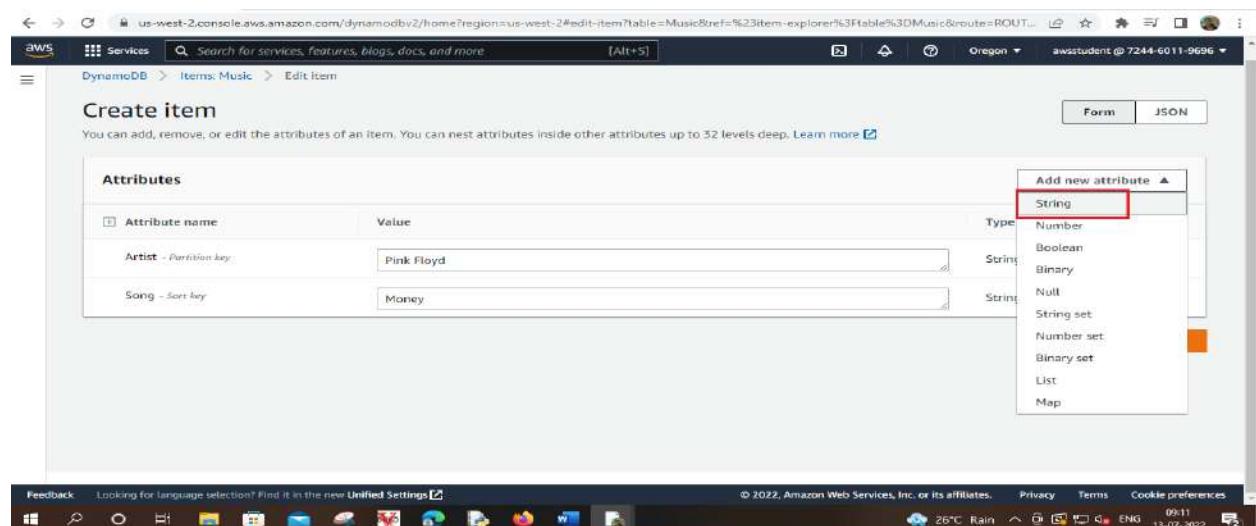
Step 13 – For Song String, type: Money.

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



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

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



A new attribute row will be added.

Step 16 – For the new attribute, enter:

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

The screenshot shows the AWS DynamoDB 'Create item' interface. A new attribute named 'Album' is being added with a value of 'The Dark Side of the Moon'. The 'Type' dropdown menu is open, showing options like String, Number, Boolean, Binary, Null, String set, Number set, Binary set, List, and Map. The 'Number' option is highlighted with a red box.

Step 17 – Add another new attribute.

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

The screenshot shows the AWS DynamoDB 'Create item' interface. A new attribute named 'Album' is being added with a value of 'The Dark Side of the Moon'. The 'Type' dropdown menu is open, and the 'Number' option is selected and highlighted with a red box.

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' dialog open. The 'Attributes' section lists four items:

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 are 'Cancel' and 'Create Item' buttons, with 'Create Item' being the active one.

Step 19 – Choose Save changes.

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

The item will appear in the console.

The screenshot shows the AWS DynamoDB console after saving an item. A green banner at the top says 'The item has been saved successfully.' The main area shows the 'Music' table with one item listed in the 'Items returned' section:

Artist	Song	Album	Year
Pink Floyd	Money	The Dark Si...	1973

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

The screenshot shows the AWS DynamoDB console after saving a second item. A red box highlights the 'Create Item' button in the toolbar. The main area shows the 'Music' table with one item listed in the 'Items returned' section:

Artist	Song	Album	Year
Pink Floyd	Money	The Dark Si...	1973

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

Attributes

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

Create item

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

Attributes

Attribute name	Value	Type
Artist - Partition key	John Lennon	String
Song - sort key	Imagine	String
Album	Imagine	String
Number	1971	Number
Genre	Soft rock	String

Create item

The screenshot shows the AWS DynamoDB console. A green banner at the top right says "The item has been saved successfully." On the left, the navigation pane shows "Tables" and "Explore items". The main area displays a table named "Music" with two items. The first item is "John Lennon" with song "Imagine" from the album "Imagine". The second item is "Pink Floyd" with song "Money" from the album "The Dark Si...". A red box highlights the "Create item" button in the top right of the table view.

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

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

The screenshot shows the "Create item" dialog in the AWS DynamoDB console. It has a "Form" tab selected. The "Attributes" section contains a table with columns for "Attribute name", "Value", and "Type". The "Artist" attribute is set to "Psy" (String). The "Song" attribute is set to "Gangnam Style" (String). The "Album" attribute is expanded, showing its value as "Psy 6 (Six Rules), Part 1" (String). The "Year" attribute is set to "2011" (Number). The "LengthSeconds" attribute is set to "219" (Number). A red box highlights the "LengthSeconds" row. A red box also highlights the "Create item" button in the bottom right corner. Red numbers "1" and "2" are placed near the highlighted areas to indicate steps.

The screenshot shows the AWS DynamoDB console. A green success message box at the top right says "The item has been saved successfully." On the left sidebar, under the "Tables" section, there is a "created" status next to the "Music" table. The main area displays the "Music" table with three items:

Artist	Song	Album	Genre	Number
Psy	Gangnam Style	Psy 6 [Six R...]		
John Lennon	Imagine	Imagine	Soft rock	1971
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 console. The "Edit item" option in the Actions menu is highlighted with a red box. The "Artist" column for the Psy item is also highlighted with a red box. The Actions menu options include: Edit item, Duplicate item, Delete items, Download selected items to CSV, and Download results to CSV.

Step 24 – Change the Year from 2011 to 2012.

The screenshot shows the AWS DynamoDB console with the 'Edit item' page for the 'Music' table. The 'Year' attribute is highlighted with a red box. Step 25 indicates to choose 'Save changes'.

Step 25 – Choose Save changes.

The screenshot shows the AWS DynamoDB console after saving changes. A green banner at the top says 'The item has been saved successfully.' The 'Music' table list shows three items with the 'Year' attribute updated to 2012.

The screenshot shows the AWS DynamoDB console with the 'Edit item' page for the 'Music' table. The 'Year' attribute is highlighted with an orange box. Step 25 indicates to choose 'Save changes'.

The item is now updated.

The screenshot shows the AWS DynamoDB console. A success message 'The item has been saved successfully.' is displayed. The 'Explore items' option in the left navigation pane is selected. The 'Music' table is shown with three items:

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...			1975

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.

The screenshot shows the AWS DynamoDB console with the 'Explore items' option highlighted in red in the left navigation pane. The 'Tables' section shows one table named 'Music' selected. The main area displays the 'Music' table with the same three items as before:

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...			1975

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 console with the 'Music' table selected. The 'Scan/Query items' section is open, showing the query configuration. The 'Query' button is highlighted with a red box. The 'Artist (Partition key)' field contains 'Psy' and the 'Song (Sort key)' field contains 'Gangnam Style'. The 'Run' button at the bottom is also highlighted with a red box. The status bar at the bottom indicates 'Completed' and 'Read capacity units consumed: 0.5'.

Step 31 – Choose Run.

The screenshot shows the results of the query. The 'Items returned (1)' section displays a single item with the following details:

Artist	Song	Album	LengthSeconds	Year
Psy	Gangnam Style	Psy 6 (Six R...	219	201

The entire table view is highlighted with a red box.

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 item has been saved successfully.

Music

Scan/Query items

Scan | Query | Music

Filters

Attribute name: Year | Type: Number | Condition: Equal to | Value: 1971 | Run | Reset

Completed | Read capacity units consumed: 0.5

Step 33 – Choose Run.

Only the song released in 1971 is displayed.

Scan/Query items

Scan | Query | Music

Filters

Attribute name: Year | Type: Number | Condition: Equal to | Value: 1971 | Run | Reset

Completed | Read capacity units consumed: 0.5

Items returned (1)

Artist	Song	Album	Genre	Year
John Lennon	Imagine	Imagine	Soft rock	1971

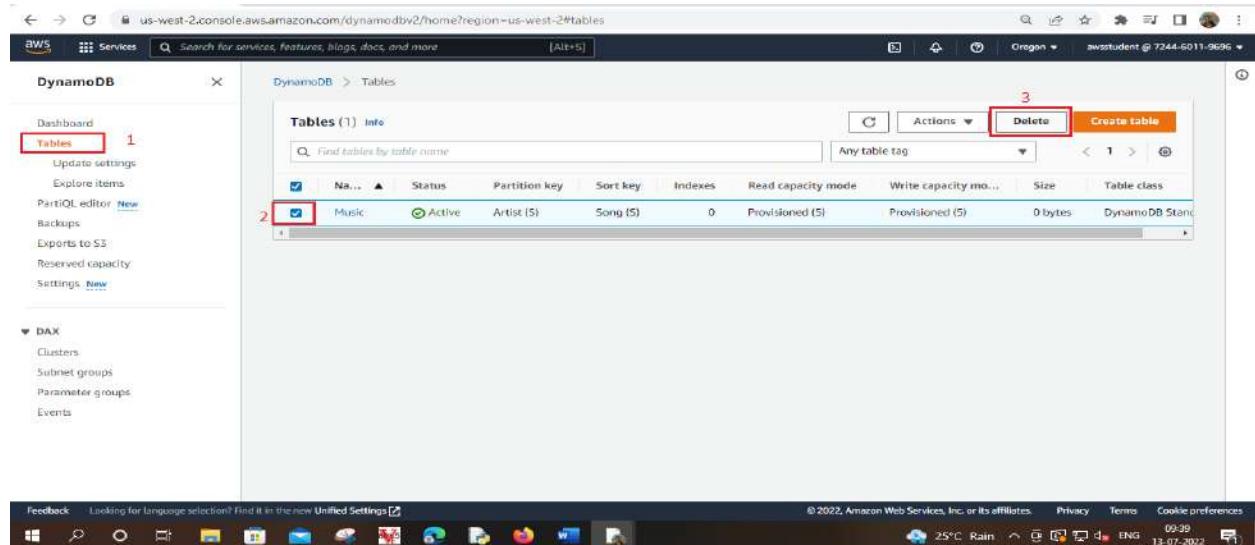
Task 5: Delete the Table

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

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

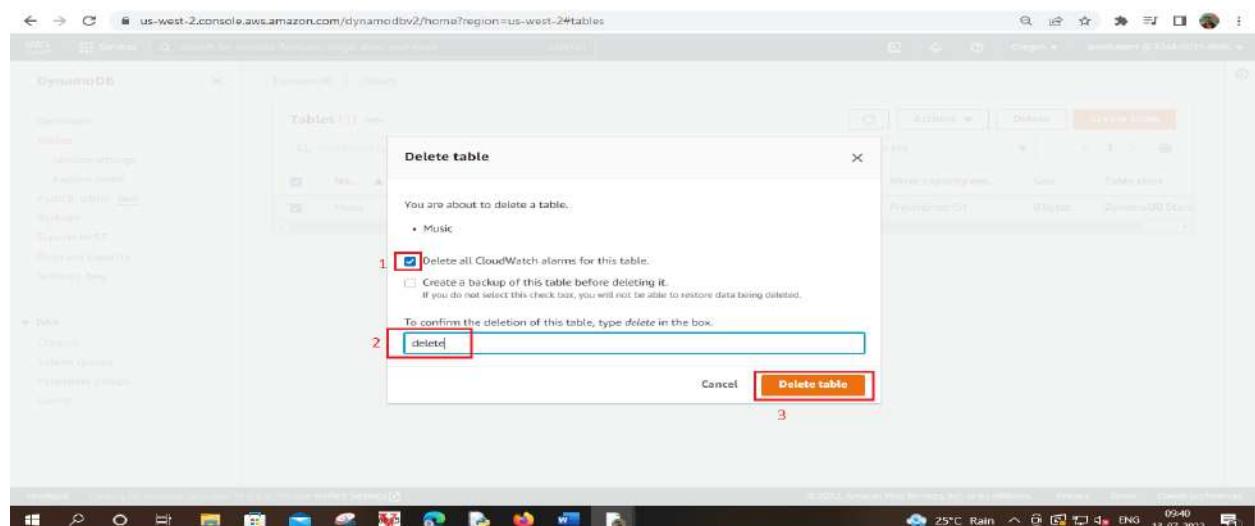
Step 35 – Choose the **Music** Tables.

Step 36 – Choose **Delete**.

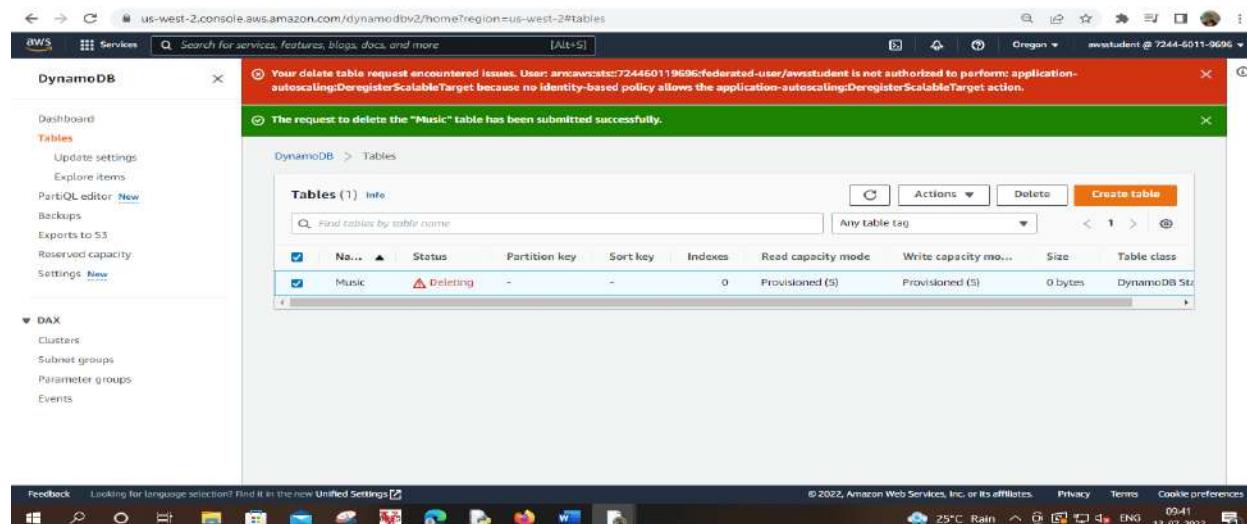


Step 37 – Enter delete.

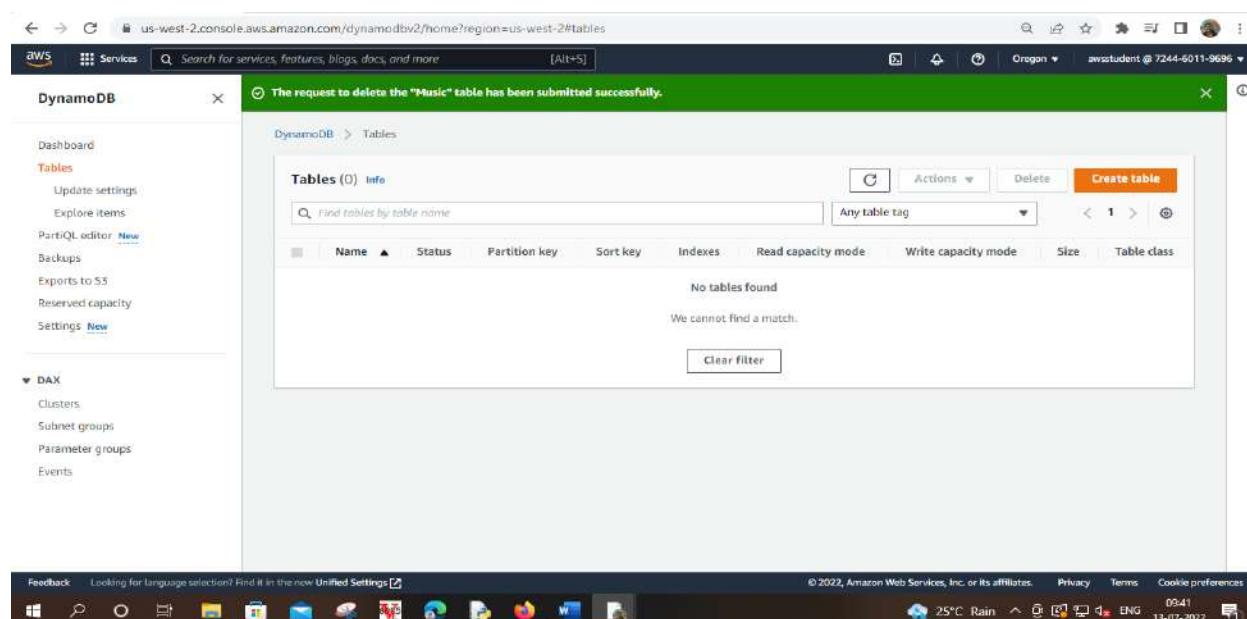
Step 38 – Choose delete table.



The table will be deleted.



Successfully deleted



Step 39 –Return to the AWS Management Console

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

Step 41 –Choose **End Lab**

Practical 6: Introduction to Amazon Redshift

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

Amazon Redshift

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

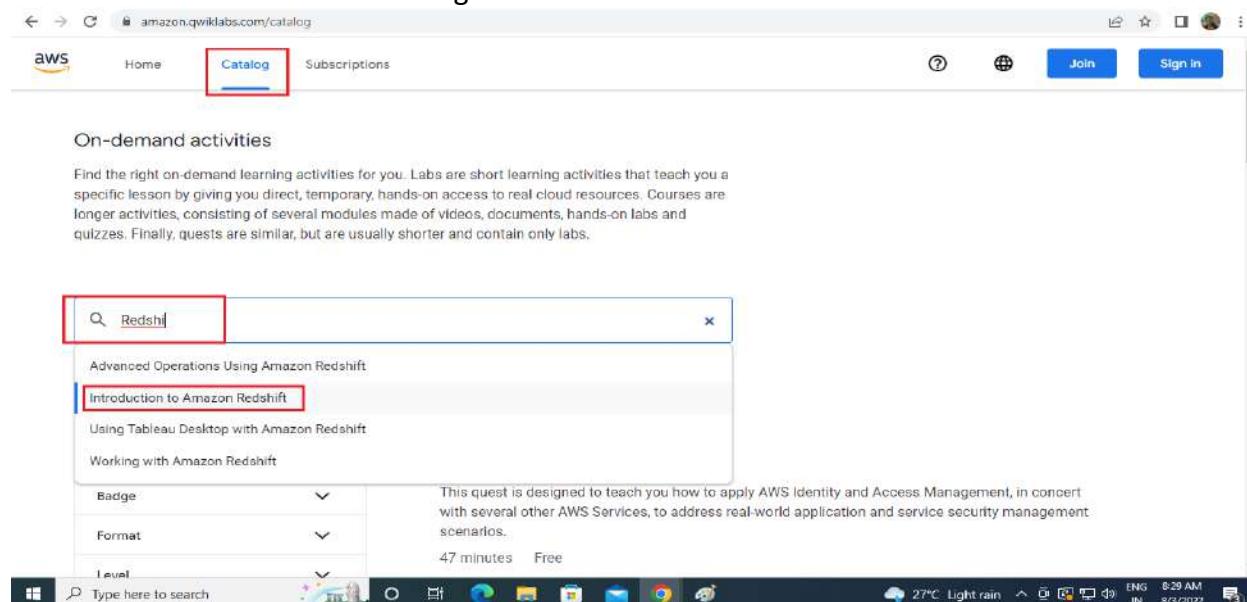
1. Creating a Redshift cluster
2. Loading data into a Redshift cluster
3. Performing queries against the data in cluster

Task 1: Launch an amazon Redshift Cluster

Step 1 – Go to the given link

<https://amazon.qwiklabs.com/catalog>

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



Step 3 – Start Lab and click on Open Console

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

Cautions: 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

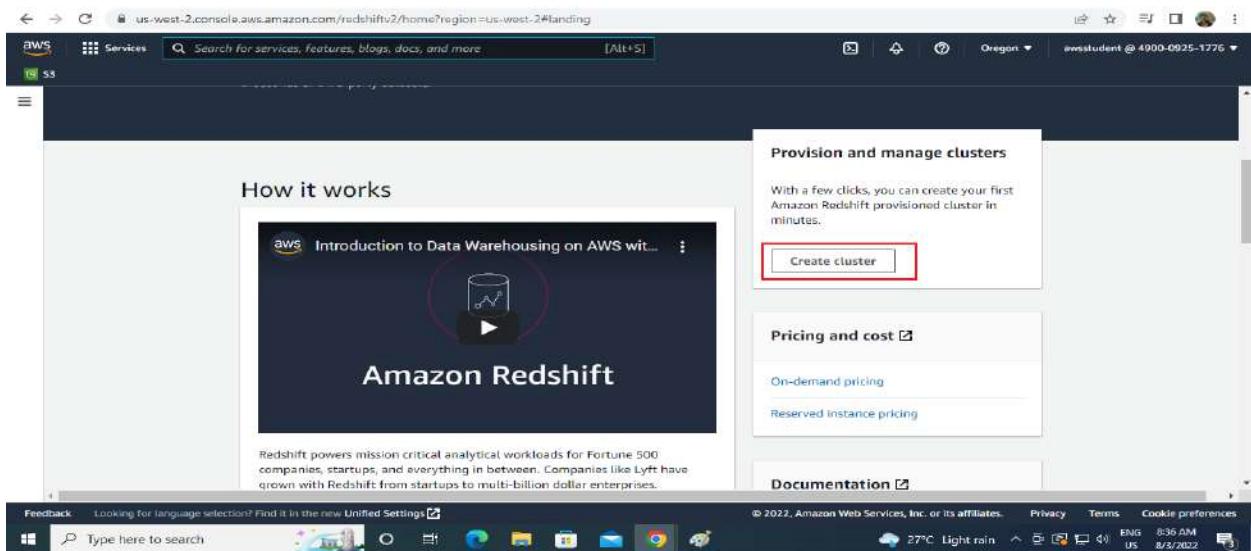
arn:aws:lambda:1498889291: /

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

Corrections, feedback, or other questions? Contact us at [AWS Training and Certification](#)

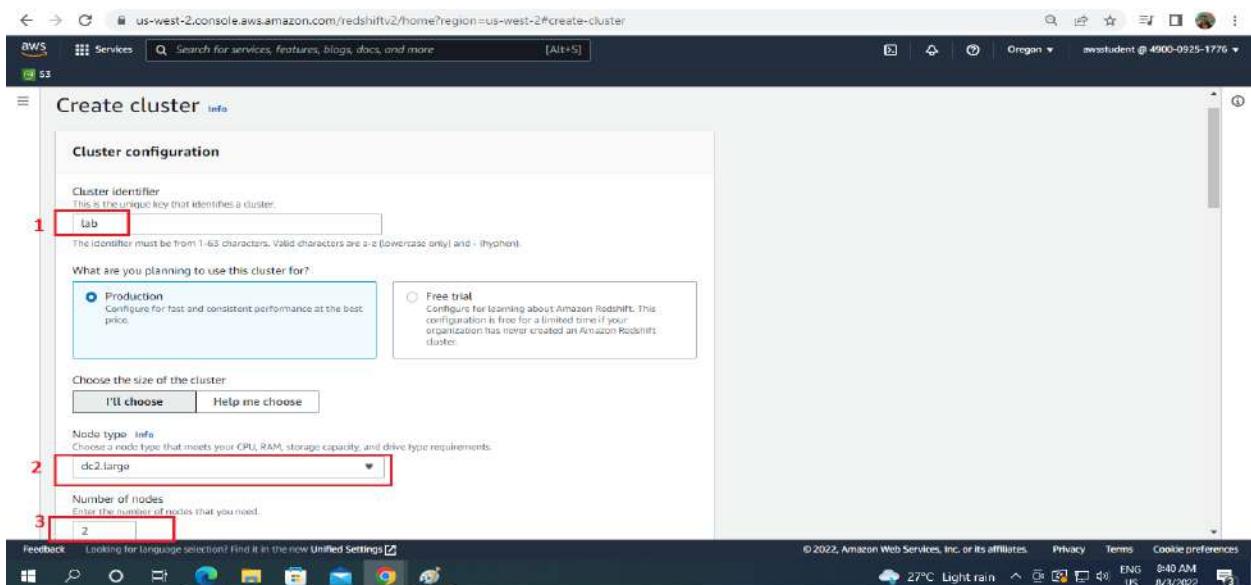
Step 4 – In the AWS Management Console, choose Services, then choose Amazon Redshift.

Step 5 – Choose Create cluster.



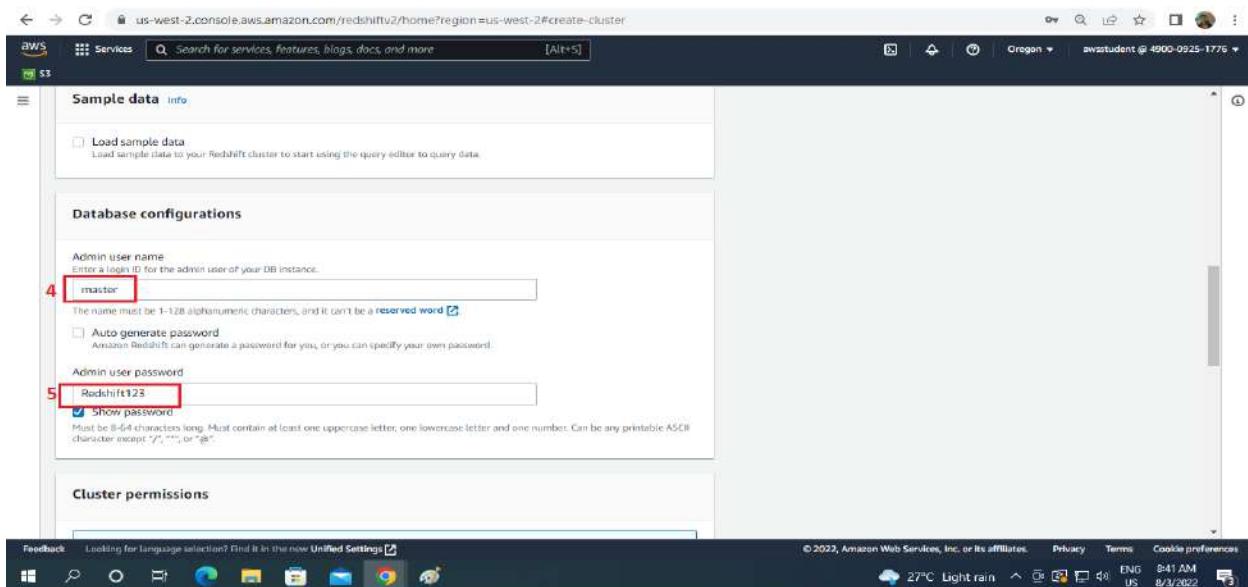
Step 6 – In the Cluster configuration section, configure:

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

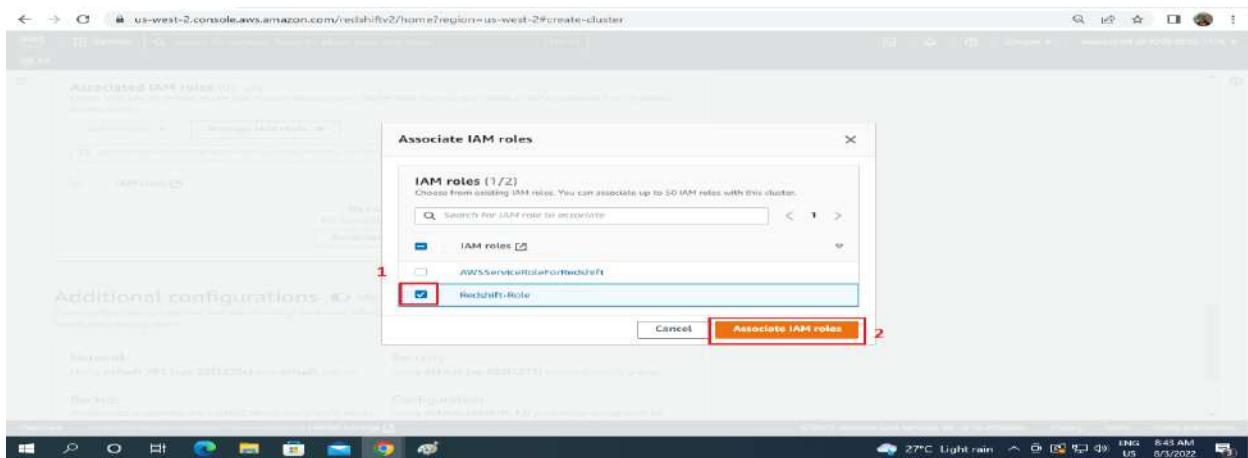
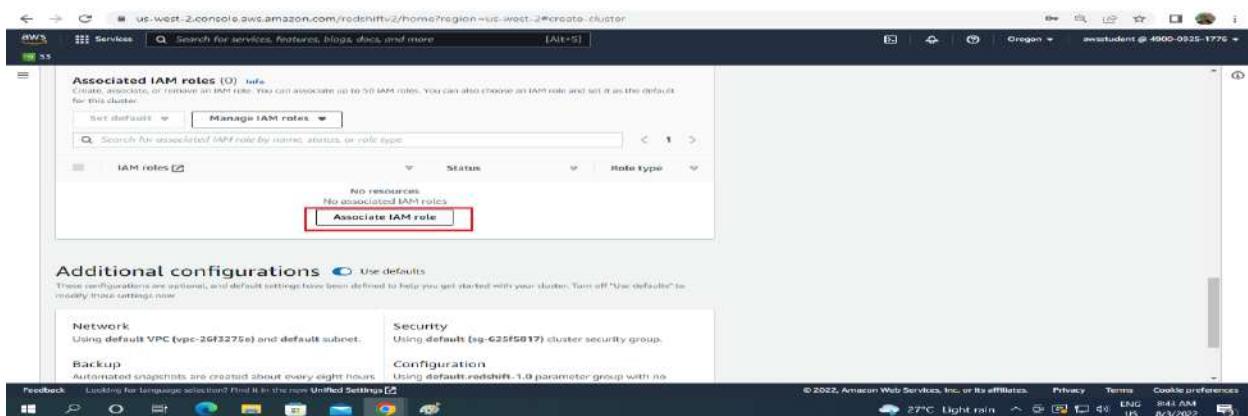


Step 7 – In the Database configurations section, configure:

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



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



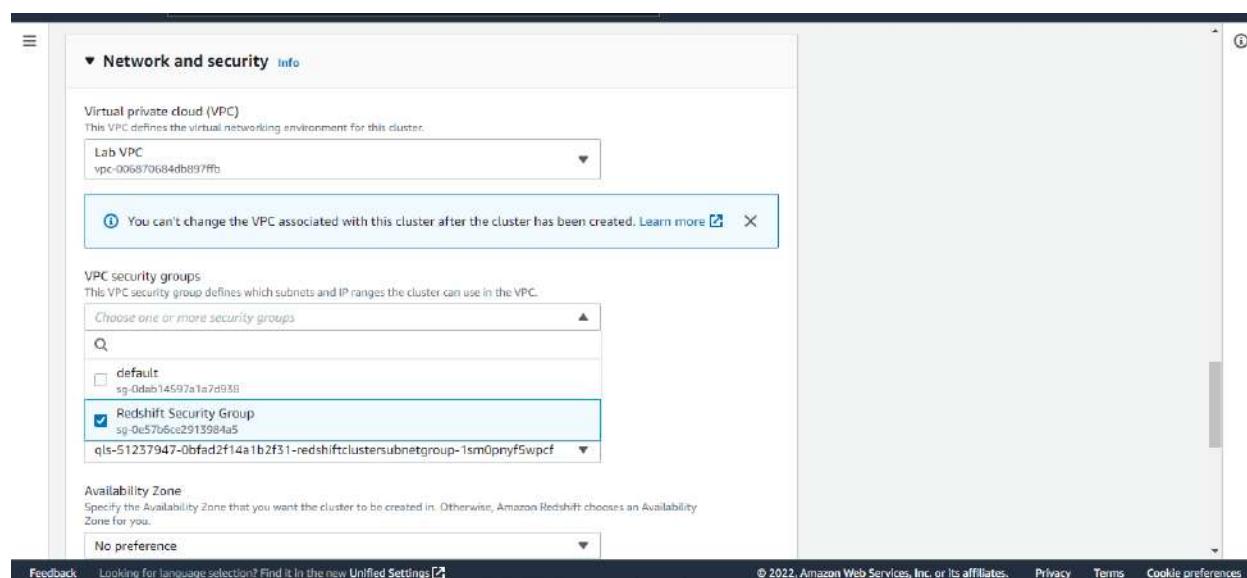
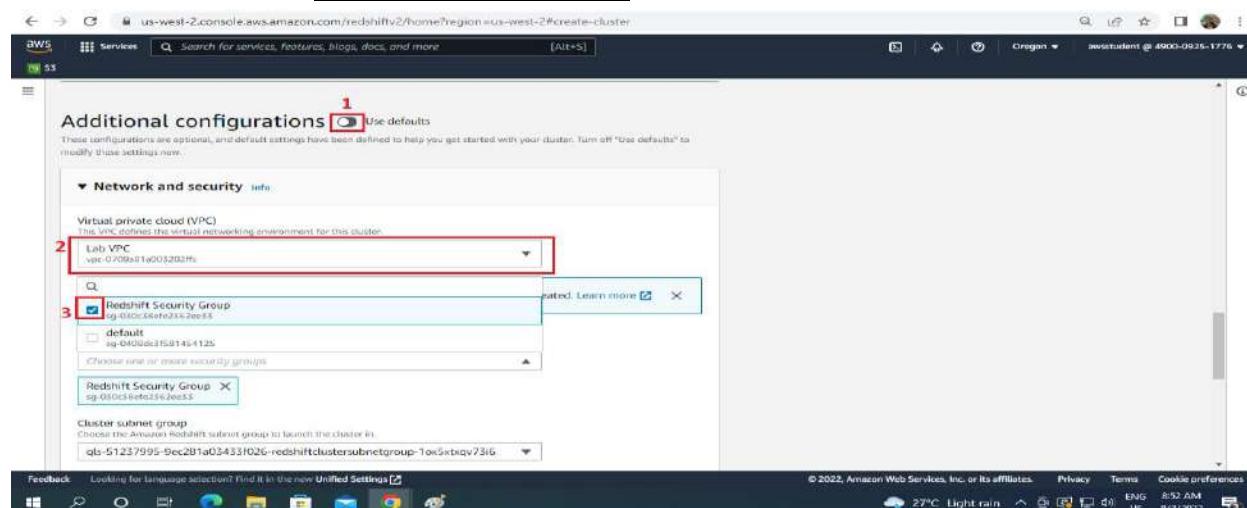
The role grants permission for Amazon Redshift to read data from Amazon S3.

Step 9 – In the Additional configurations section,

1. Deselect Use defaults

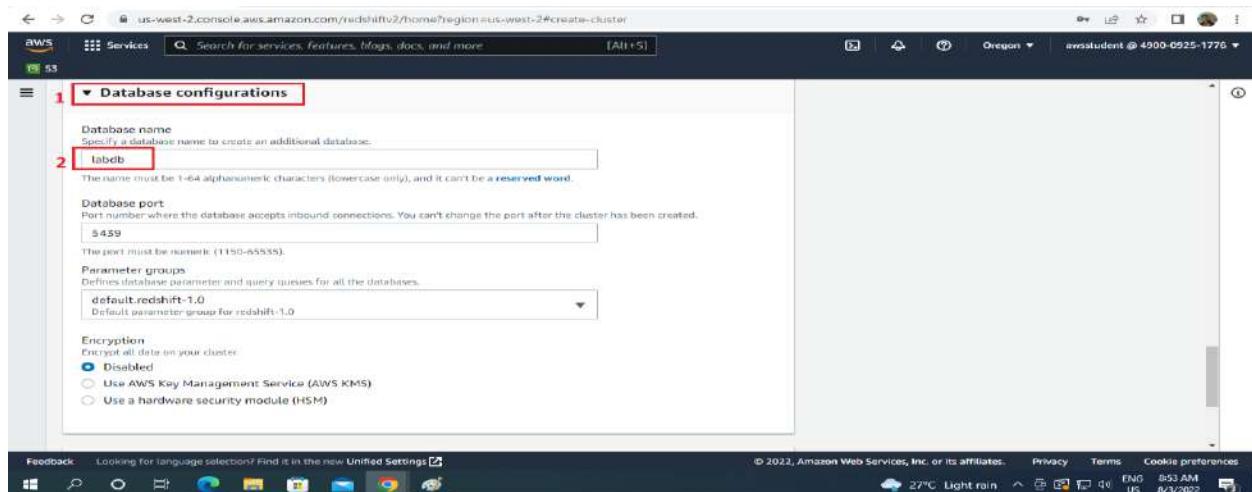
Expand Network and security, then configure:

- Virtual private cloud: Lab VPC
- VPC security groups:
 - **Deselect Use default**
 - **Check or select Redshift Security Group.**

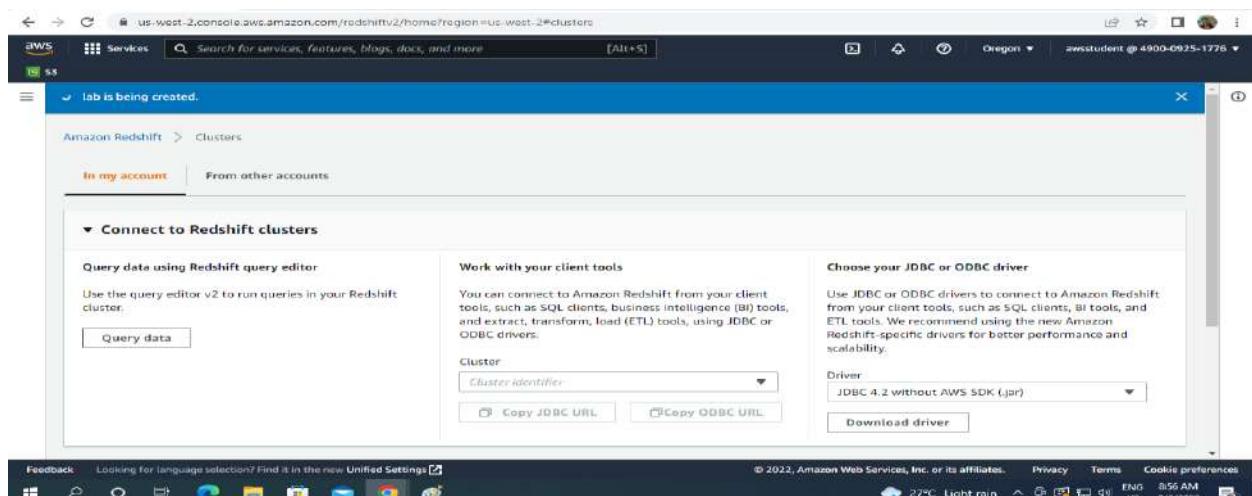
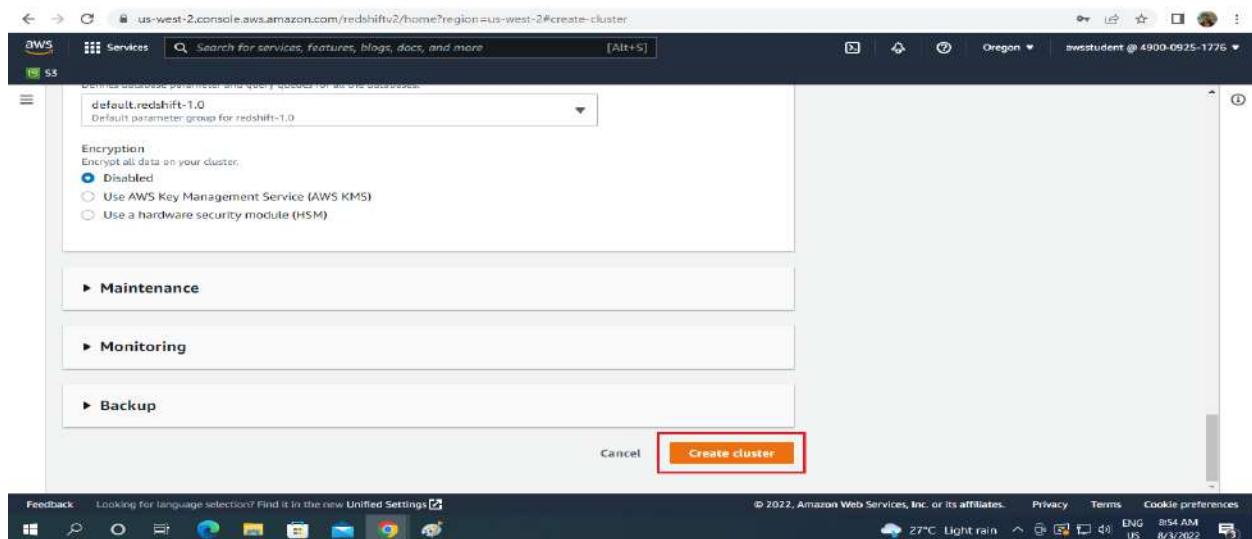


Step 10 – Expand Database configurations, then configure:

- Database name: labdb



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



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

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

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

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

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

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

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

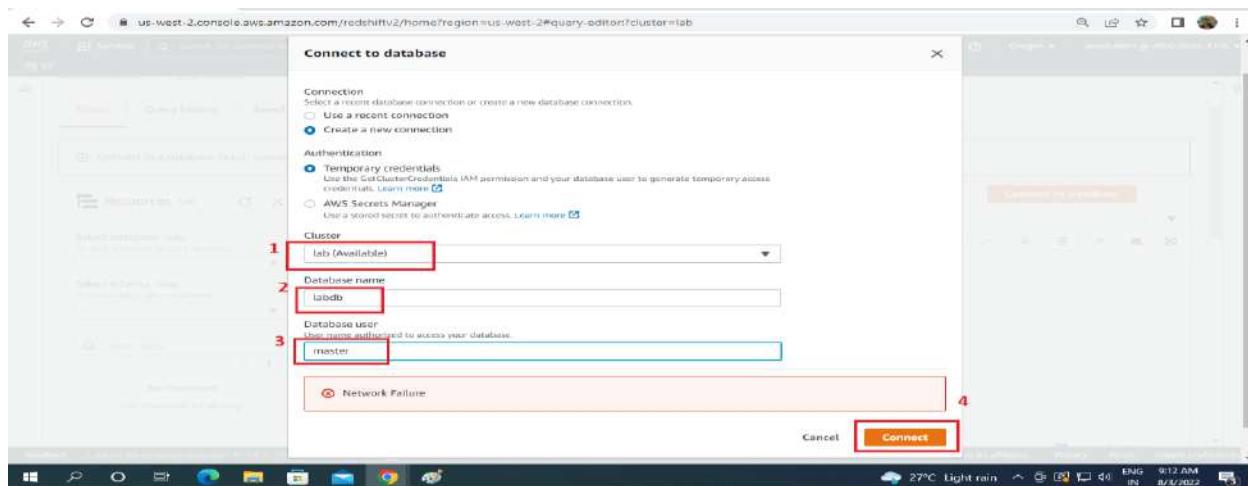
- **Cluster:** lab
- **Database name:** labdb
- **Database user:** masterStep

The screenshot shows the AWS Management Console for Amazon Redshift. The URL is us-west-2.console.aws.amazon.com/redshiftv2/home?region=us-west-2#cluster-details?cluster=lab. The page displays information about the 'lab' cluster, including its identifier, status, node type, number of nodes, and endpoint. At the top right, there are buttons for 'Actions', 'Edit', 'Add partner integration', and two red-highlighted buttons: 'Query in query editor' and 'Query in query editor v2'. Below the main content, there's a feedback link and a footer with copyright information and weather details.

Step 13 – Click Connect to database

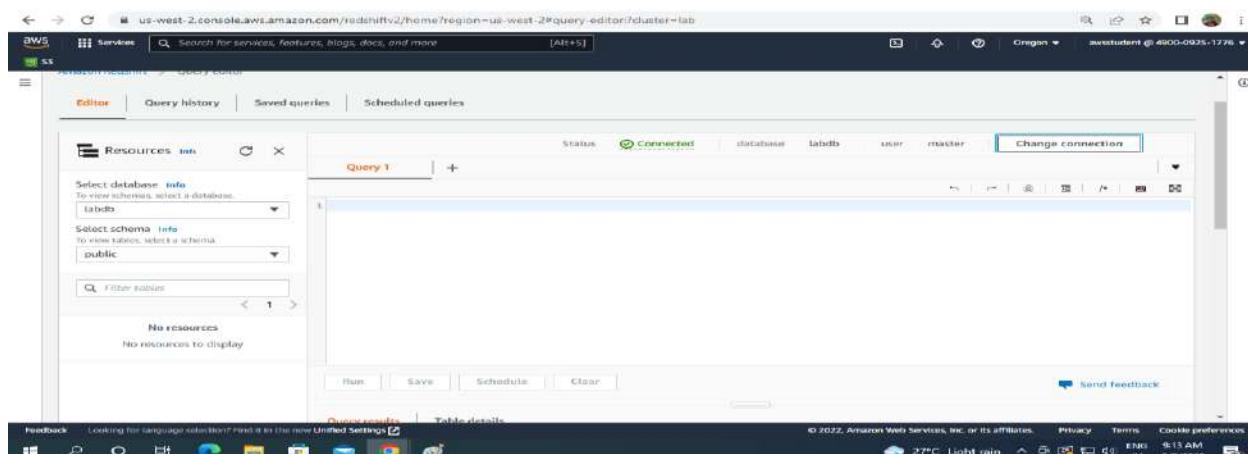
The screenshot shows the AWS Management Console for the Redshift Query Editor. The URL is us-west-2.console.aws.amazon.com/redshiftv2/home?region=us-west-2#query-editor?cluster=lab. The page has tabs for 'Editor', 'Query history', 'Saved queries', and 'Scheduled queries'. It features a 'Resources' sidebar with dropdowns for 'Select database' and 'Select schema', and a 'Filter tables' search bar. A red-highlighted 'Connect to database' button is located at the top right of the main query area. The footer includes standard AWS links and a weather forecast.

Step 14 – Click Connect button.



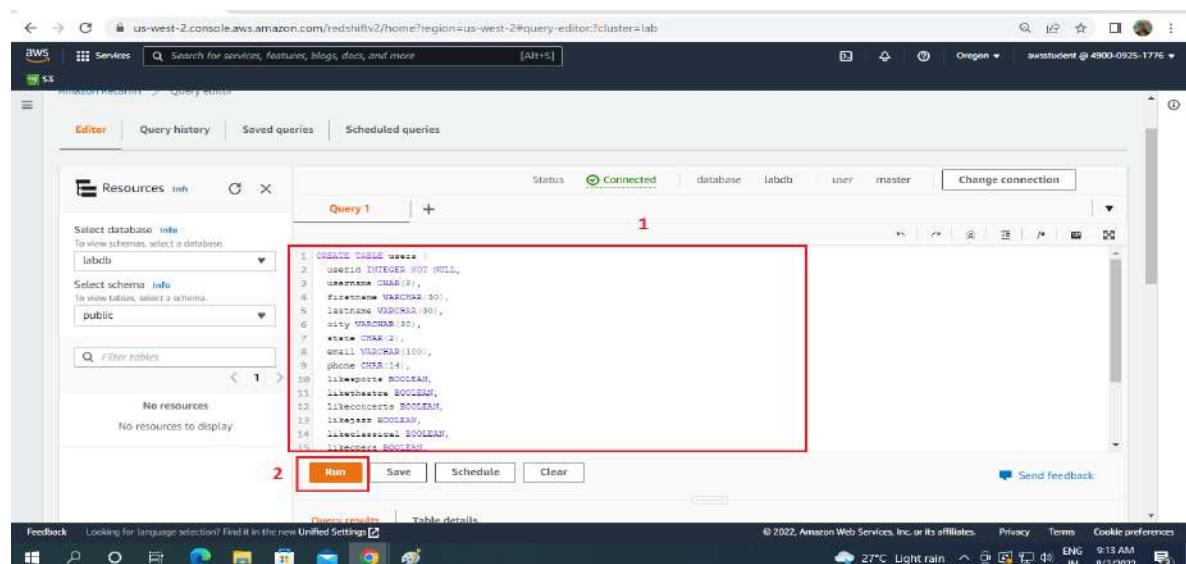
Task 3: Create a Table

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



```

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



The screenshot shows the AWS Redshift Query Editor interface. On the left, there's a sidebar with 'Resources' and 'Services' tabs, and a search bar. Below that, it says 'Select database: info' and 'Select schema: info'. A 'Filter tables' input field contains the text 'users'. The main area is titled 'Query 1' and contains the following SQL code:

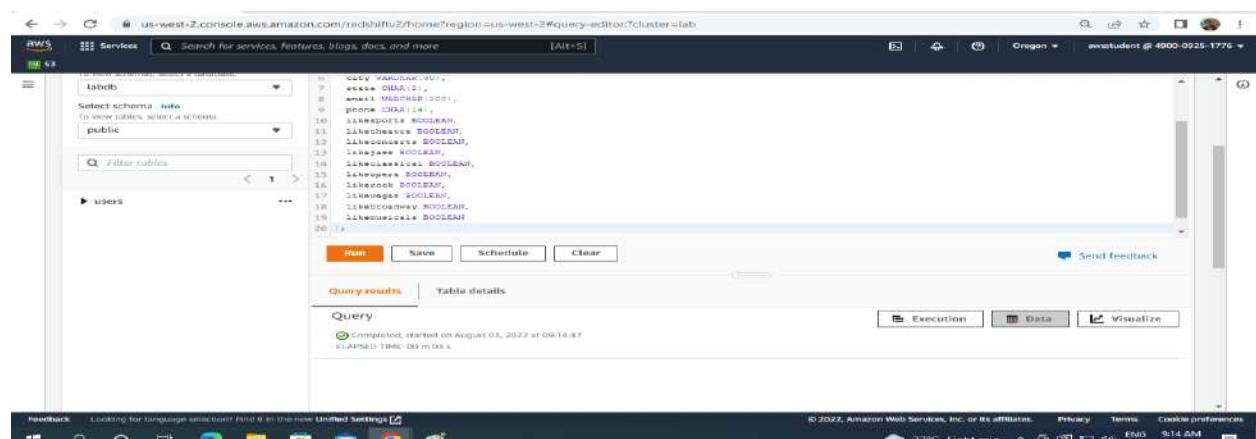
```

1 CREATE TABLE users
2   user_id INTEGER NOT NULL,
3   username CHAR(1),
4   first_name VARCHAR(30),
5   last_name VARCHAR(30),
6   email VARCHAR(32),
7   phone CHAR(14),
8   likepopcorn BOOLEAN,
9   likecartoon BOOLEAN,
10  liketheatre BOOLEAN,
11  likeconcerts BOOLEAN,
12  likeguitar BOOLEAN,
13  likeclassical BOOLEAN,
14  likecountry BOOLEAN
15

```

Below the code, there are four buttons: 'Run', 'Save', 'Schedule', and 'Clear'. The 'Run' button is highlighted with a red box. At the bottom of the editor, there are tabs for 'Query results' and 'Table details'. The status bar at the bottom right shows '© 2022, Amazon Web Services, Inc. or its affiliates.' and the date '8/3/2022'.

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



The screenshot shows the AWS Redshift Query Editor interface after running the previous query. The 'Query results' tab is selected. The results show the structure of the 'users' table:

```

1 CREATE TABLE users
2   user_id INTEGER NOT NULL,
3   username CHAR(1),
4   first_name VARCHAR(30),
5   last_name VARCHAR(30),
6   email VARCHAR(32),
7   phone CHAR(14),
8   likepopcorn BOOLEAN,
9   likecartoon BOOLEAN,
10  liketheatre BOOLEAN,
11  likeconcerts BOOLEAN,
12  likeguitar BOOLEAN,
13  likeclassical BOOLEAN,
14  likecountry BOOLEAN,
15

```

At the bottom of the results, it says 'Compilation started on August 04, 2022 at 09:14:07' and 'ELAPSED: 1040.00 m 0.0 s'. There are also buttons for 'Execution', 'Data', and 'Visualize'.

The screenshot shows the AWS DynamoDB console with a table named 'Music'. The table structure includes columns for Artist, Song, Album, Genre, and Year. A single item is displayed: John Lennon, Imagine, Imagine, Soft rock, 1971.

	Artist	Song	Album	Genre	Year
	John Lennon	Imagine	Imagine	Soft rock	1971

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::

Challenge

Try to write a query for these requirements:

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

Try to do it yourself before seeing the answer.

If you do not know the answer, [view the answer here](#).

Conclusion

Congratulations! You have completed the lab. During the lab you successfully:

https://amazon.qwiklabs.com/focuses/41510?catalog_rank=%7B%22rank%22%3A1%2C%22num_filters%22%3A0%2C%22has_search%22%3Atrue%2D%22parent_catalog%22%3A1%2C%22search_id%22%3A17667944

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

Step 19 – Click Run button

```
1. COPY users FROM 's3://aws-samples-dbus-west2/ticket/allusers_pipe.txt'
2. CREDENTIALS 'aws_iam_role=arn:aws:iam::490009281776:role/Redshift-Role'
3. DELIMITER '!';
```

Run **Save** **Schedule** **Clear**

Query results **Table details**

Query 309 Execution Data Visualize

Completed, started on August 05, 2022 at 09:18:06
ELAPSED TIME: 00 m 09 s

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. A red box highlights the SQL query: `SELECT COUNT(*) FROM users;`. Another red box highlights the 'Run' button. The results section shows the output of the query: `Query 309` completed at 09:18:54 with an elapsed time of 00 m 37 s. The result table has one row with the value `49990`.

This screenshot is identical to the one above, showing the AWS Redshift Query Editor interface. A red box highlights the SQL query: `SELECT COUNT(*) FROM users;`. Another red box highlights the 'Run' button. The results section shows the output of the query: `Query 344` completed at 09:19:41 with an elapsed time of 00 m 02 s. The result table has one row with the value `49990`.

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 Redshift Query Editor interface. A red box highlights the SQL query in the 'Query 1' editor:

```

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

A red box also highlights the 'Run' button below the query editor.

The results section shows 'Query 344' completed, with 18 rows returned. The results table is as follows:

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
12427	Haley	Wells	New York	OH

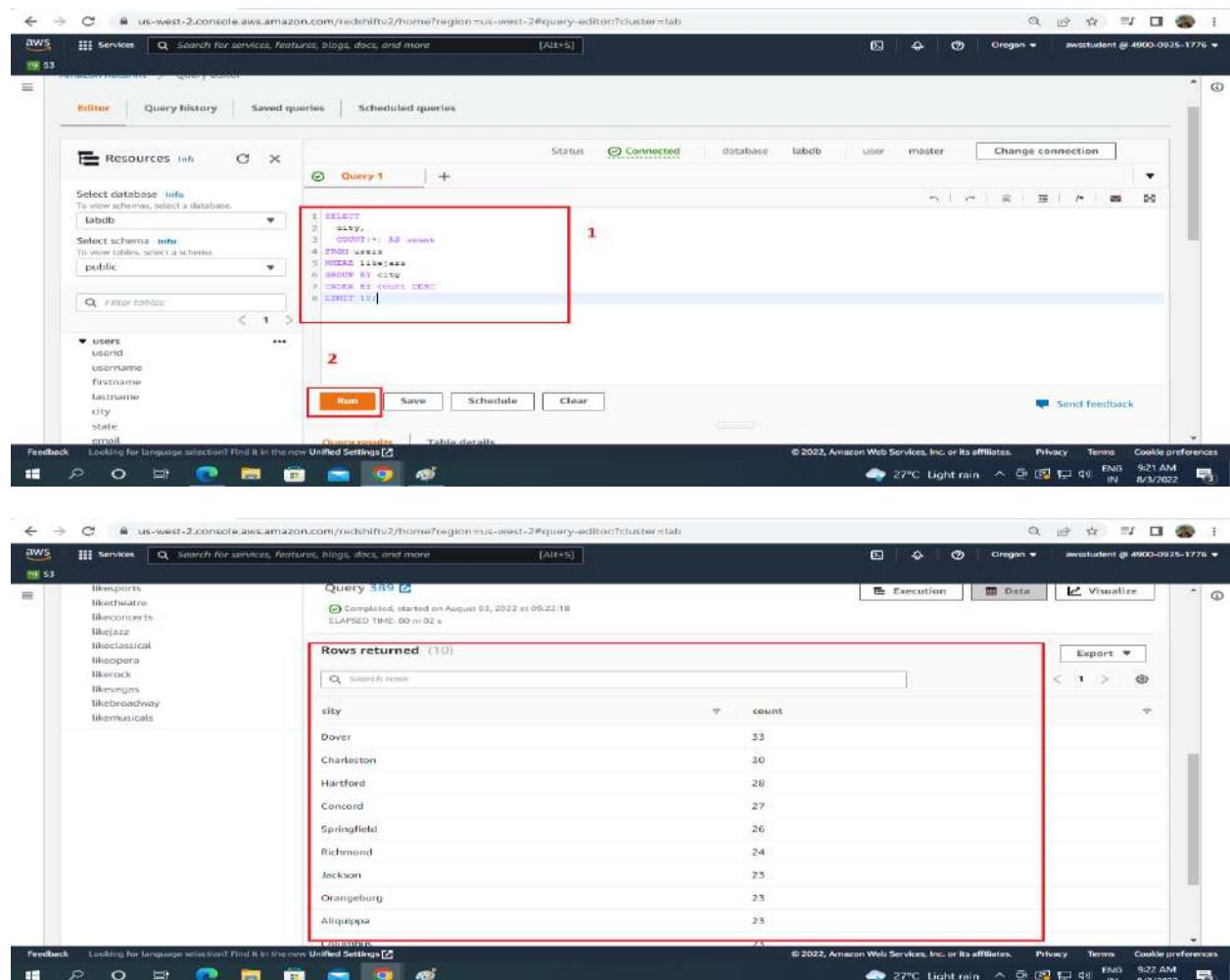
This query displays users in Ohio (OH) who like sports but do not like opera. The list is sorted by their first name.

The screenshot shows the AWS Redshift Query Editor interface. A red box highlights the results table titled 'Rows returned (18)'.

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
12427	Haley	Wells	New York	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 Redshift Query Editor interface. In the top navigation bar, there are tabs for 'Editor', 'Query history', 'Saved queries', and 'Scheduled queries'. Below the tabs, there are dropdown menus for 'Select database' (set to 'labdb') and 'Select schema' (set to 'public'). A search bar labeled 'Filter tables' is also present.

In the main area, a query is displayed in the editor:

```

1 SELECT
2   city,
3   COUNT(*) AS count
4 FROM users
5 WHERE likes_jazz
6 GROUP BY city
7 ORDER BY count DESC
8 LIMIT 10;

```

The first line of the query is highlighted with a red box and labeled '1'. The run button is highlighted with a red box and labeled '2'.

Below the editor, there are buttons for 'Run', 'Save', 'Schedule', and 'Clear'. To the right, there are links for 'Send feedback', 'Execution', 'Data', and 'Visualize'. The status bar at the bottom indicates the query was compiled on August 03, 2022, at 05:22:18, with an elapsed time of 60 ms 02 s.

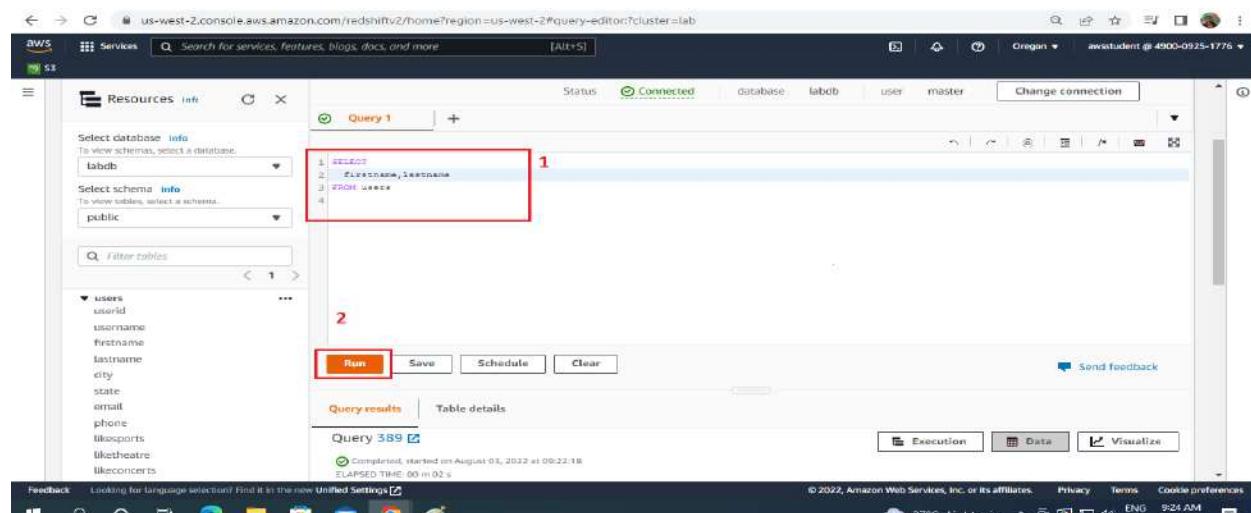
The results section shows a table titled 'Rows returned (10)'. The table has two columns: 'city' and 'count'. The data is as follows:

city	count
Dover	33
Charleston	30
Hartford	28
Concord	27
Springfield	26
Richmond	24
Jackson	23
Orangeburg	23
Albuquerque	23

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



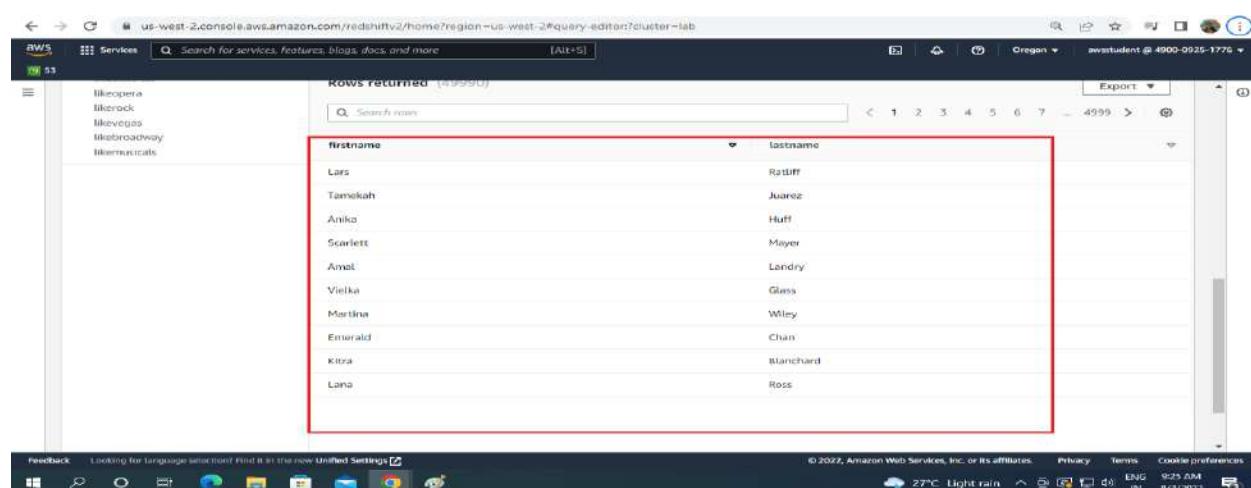
The screenshot shows the AWS Redshift Query Editor interface. A red box highlights the SQL query in the editor:

```

1: SELECT
2:   firstname, lastname
3: FROM users
4:

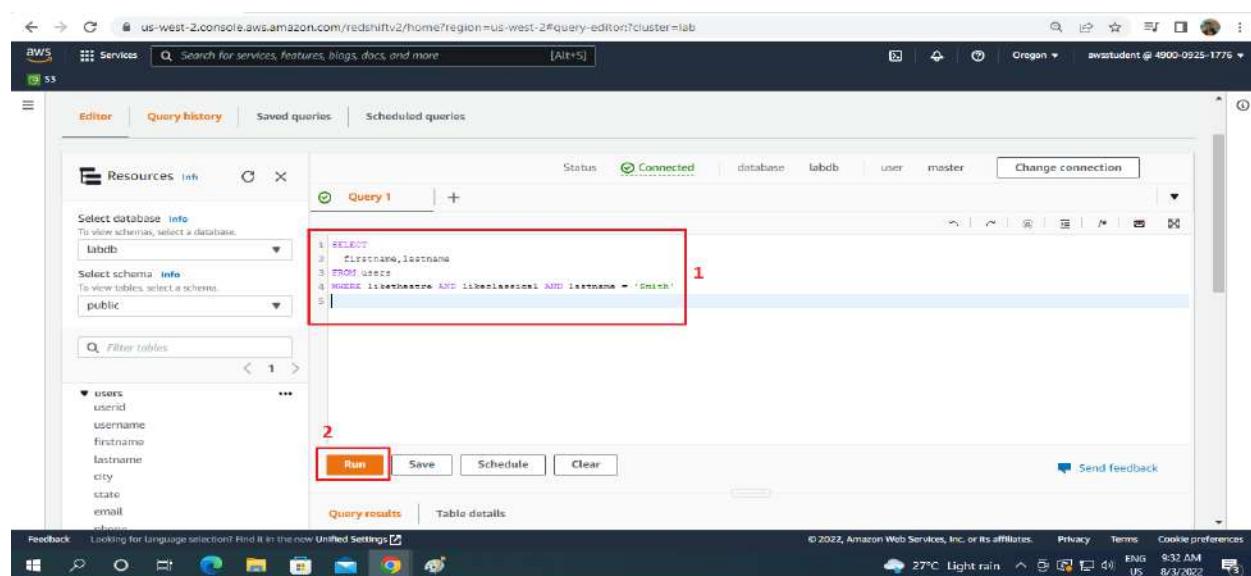
```

Below the editor, a red box highlights the "Run" button. The results pane shows a table with two columns: "firstname" and "lastname". The table has 4999 rows.



The screenshot shows the results of the query execution. A red box highlights the results table:

firstname	lastname
Lars	Ratiff
Tamikah	Juarez
Anika	Huff
Scarlett	Mayer
Amel	Londry
Vielka	Glass
Martina	Wiley
Emerald	Chan
Kitra	Blanchard
Lana	Ross



The screenshot shows the AWS Redshift Query Editor interface. A red box highlights the SQL query in the editor:

```

1: SELECT
2:   firstname, lastname
3: FROM users
4: WHERE likeopera AND likerock AND lastname = 'Smith'
5:

```

Below the editor, a red box highlights the "Run" button. The results pane shows a table with two columns: "firstname" and "lastname". The table has 1 row.

The screenshot shows the AWS Management Console interface for a Redshift cluster. On the left, there's a sidebar with various database names listed. The main area displays a table titled 'Rows returned (4)'. The table has two columns: 'firstname' and 'lastname'. The data is as follows:

firstname	lastname
Wade	Smith
Berke	Smith
Aline	Smith
Lionel	Smith

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

This screenshot shows the AWS Management Console with the user profile dropdown open. The dropdown menu includes options like 'Account', 'Organization', 'Service Quotas', 'Billing Dashboard', and 'Settings'. At the bottom right of the dropdown, there is a 'Sign out' button, which is highlighted with a red box.

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

This screenshot shows the 'End lab' step in the Amazon Qwiklabs lab process. A confirmation dialog box is displayed, asking if the user wants to end the lab. It states: 'All done? If you end this lab, you will lose all your work. You may not be able to restart the lab if there is a quota limit. Are you sure you want to end this lab?' There are 'Cancel' and 'Submit' buttons at the bottom of the dialog. The 'Submit' button is highlighted with a red box.

Practical 7: Introduction to AWS device Farm

- A. Create KMS master key Locate or Download an Example Android * .apk and iOS *.ipa File**
- B. Upload and Test the Example Application**
- C. Run Test and View the Run's Results**

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

Step 1 – Go to the given link

https://amazon.qwiklabs.com/focuses/37983?catalog_rank=%7B%22rank%22%3A13%2C%22num_filters%22%3A1%2C%22has_search%22%3Atrue%7D&parent=catalog&search_id=17288638

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

The screenshot shows a web browser window with the URL 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. The page title is "Introduction to AWS Device Farm". On the left, there is a "Start Lab" button and a timer showing "00:45:00". In the center, there is an "aws training and certification" logo with "45 minutes" and "Free" next to it. A 5-star rating icon is also present. Below the logo, it says "SPL-27 - Version 1.5.11". To the right, there is a sidebar with links: 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, and Additional Resources. At the bottom of the browser window, there is a taskbar with various icons and system status information like "27°C Rain", "ENG IN", and the date "8/10/2022".

Step 3 – Download one of the following files.

The screenshot shows a browser window for the AWS Device Farm lab. At the top, there's a red button labeled "End Lab" and a timer showing "00:43:06". A message says, "you would like to use for this lab to test, locate the compiled *.apk or *.ipa at this time." Below this, a note cautions against deviating from lab instructions. A "Learn more" link is present. A "Open Console" button is visible. To the right, a sidebar lists navigation links: 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, and Additional Resources. The main content area contains numbered steps: 3. Please download one of the following files to your computer, with three links listed: [flickrj-android-sample-android.apk](#), [mixarev0.9.2.apk](#), and [github.com/mehtank/androminion/releases](#). Step 4. In the AWS Management Console, on the Services menu, click Device Farm. Step 5. If you see Next, click it. Step 6. At the AWS Device Farm window, configure: Project Name: myProject, Click Create. A note below says: If you type a project name other than myProject, be sure to use it consistently throughout this lab.

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

The screenshot shows a browser window displaying the Google Code Archive page for the project "flickrj-android". The URL is code.google.com/archive/p/flickrj-android/downloads. The page lists several versions of the project, including "sources.jar" and "flickrj-android-sample-android.apk". The "flickrj-android-sample-android.apk" file is highlighted with a red border. The file details are: Binary Bundle(excluding dependencies) Release 1.0.3.20120619135416, Jun 19, 2012, 318.91KB. The status is "Type-Archive". Other files listed include "flickrj-android-1.0.2.20120411195700-sources.jar", "flickrj-android-1.0.2.20120411195700.jar", "flickrj-android-1.0.1.20111224194607-sources.jar", "flickrj-android-1.0.1.20111224194607.jar", "flickrj-android-1.0.0.2011122213155-sources.jar", and "flickrj-android-1.0.0.2011122213155.jar". The status for most files is "Deprecated". The bottom of the screen shows a taskbar with various icons and a system tray indicating 27°C Rain, ENG 8:44 AM, IN 8/10/2022.

Step 5 – Click on Open Console button.

End Lab 00:44:44

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](#)

45 minutes Free ★★★★☆

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

27°C Rain ENG 8:47 AM IN 8/10/2022

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

Services (63)

Device Farm

Search results for 'device'

Services

Device Farm

Test Android, iOS, and Web Apps on Real Devices in the Cloud

IoT Device Management

Securely Manage Fleets as Small as One Device, or as Broad as Millions of Devices

IoT Device Defender

Secure your fleet of connected IoT devices

AWS Panorama

Enabling computer vision applications at the edge

Features

Device logs

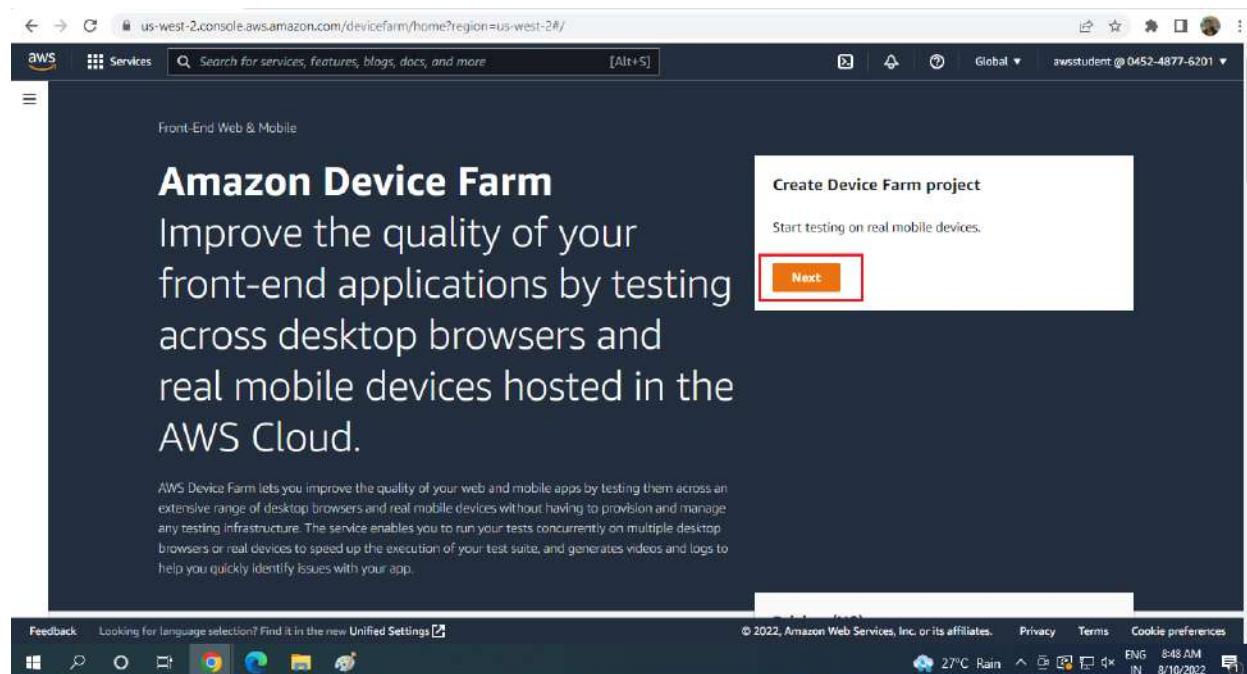
IoT Core feature

https://console.aws.amazon.com/devicefarm/home?region=us-west-2

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

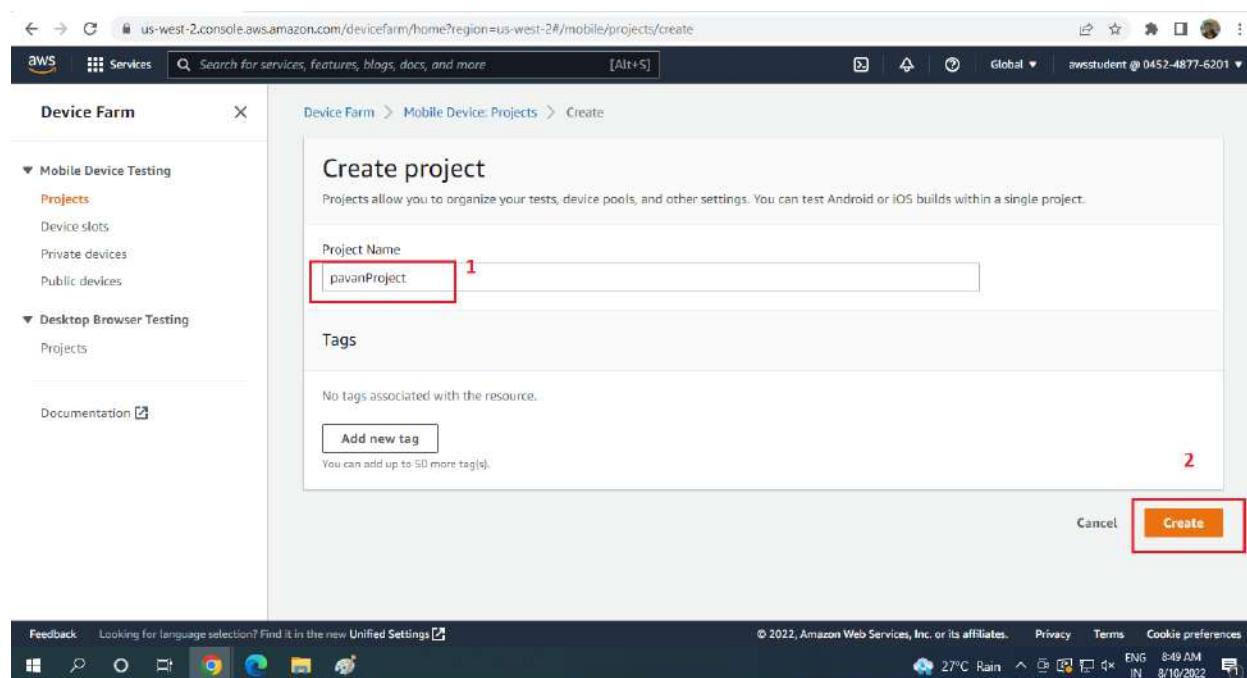
27°C Rain ENG 8:47 AM IN 8/10/2022

Step 7 – Click on **Next** button.



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

Project name: **pavanProject**



New project is created.

The screenshot shows the AWS Device Farm console interface. At the top, there's a banner message: "Successfully created mobile project *pavanProject*." The left sidebar has sections for "Mobile Device Testing" (Projects, Device slots, Private devices, Public devices) and "Desktop Browser Testing" (Projects). Below the sidebar is a "Documentation" link. The main content area shows the "pavanProject" details, including its Project ARN: arn:aws:devicefarm:us-west-2:045248776201:project:84ccb1ed-df31-4a41-b6b2-b1e7c8d28327. It features tabs for "Automated tests" (selected) and "Remote access". A note says: "Automated runs allow you to execute built-in tests or your own scripts on one or more devices in parallel, which generates a comprehensive report that includes high-level results, logs, screenshots, and performance data." A prominent orange button says "Create a new run". Below it is a table header for "Status", "Name", "Test results", "Test type", "Created", and "Total time". A message at the bottom says: "You don't have any automated runs yet." and "No resources to display." The bottom of the screen shows the Windows taskbar with various icons and system status information.

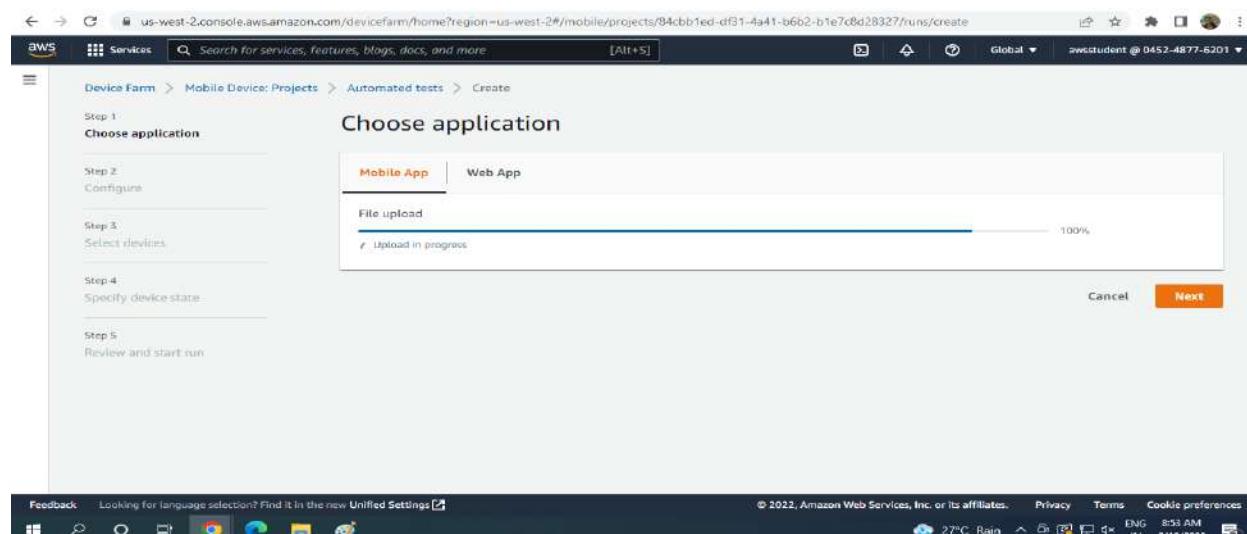
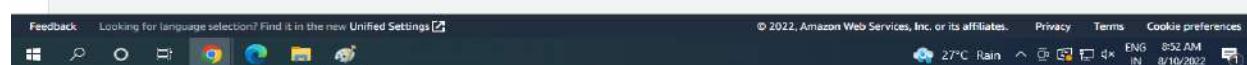
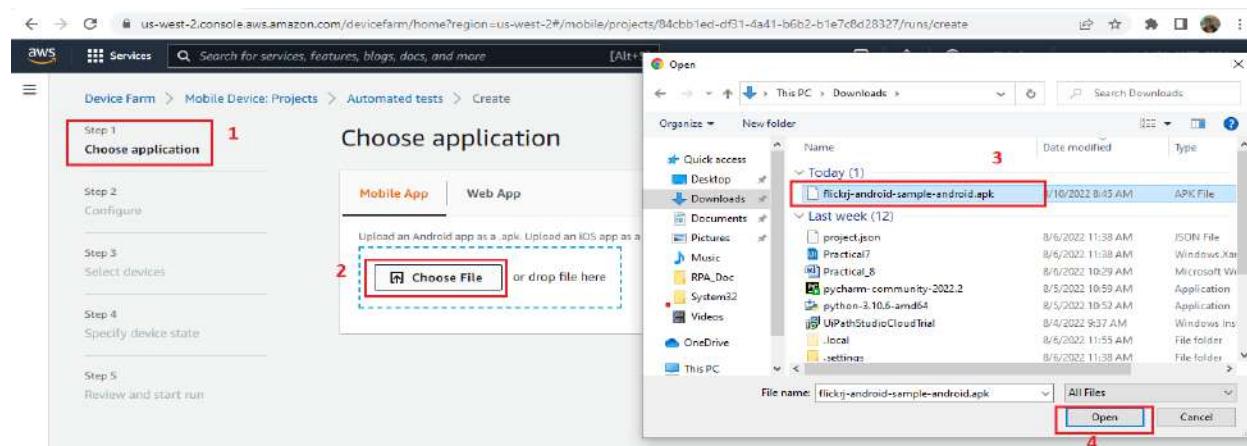
Task 2: Upload and Test the Example Application

Step 9 – Click Create a new run

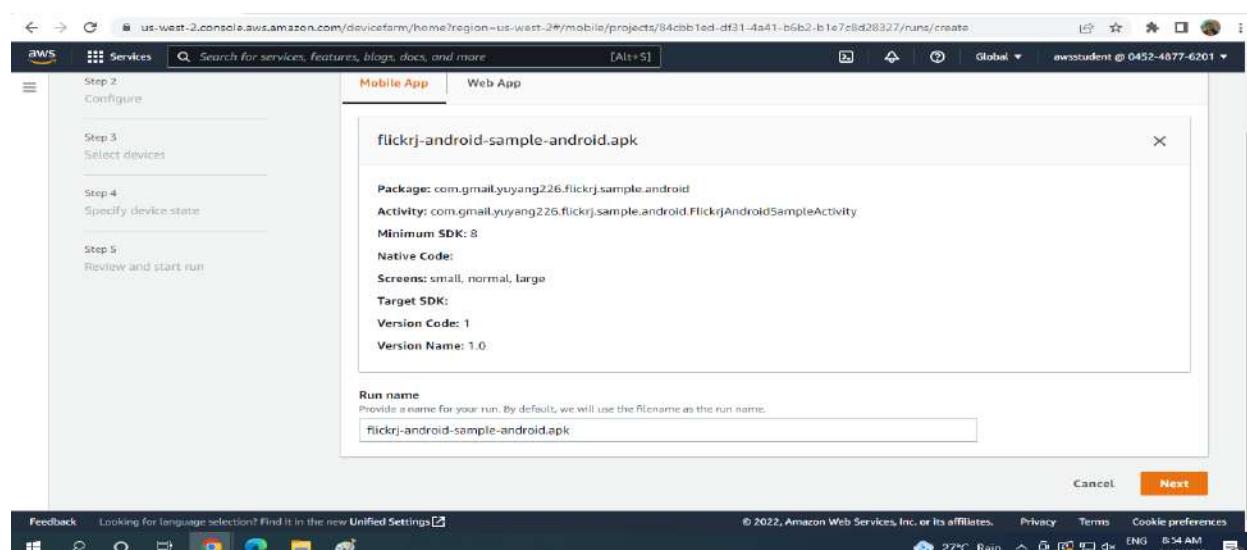
This screenshot is identical to the one above, showing the AWS Device Farm console with the "pavanProject" page. The "Create a new run" button is highlighted with a red box. The rest of the interface, including the sidebar, project details, and table, remains the same.

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

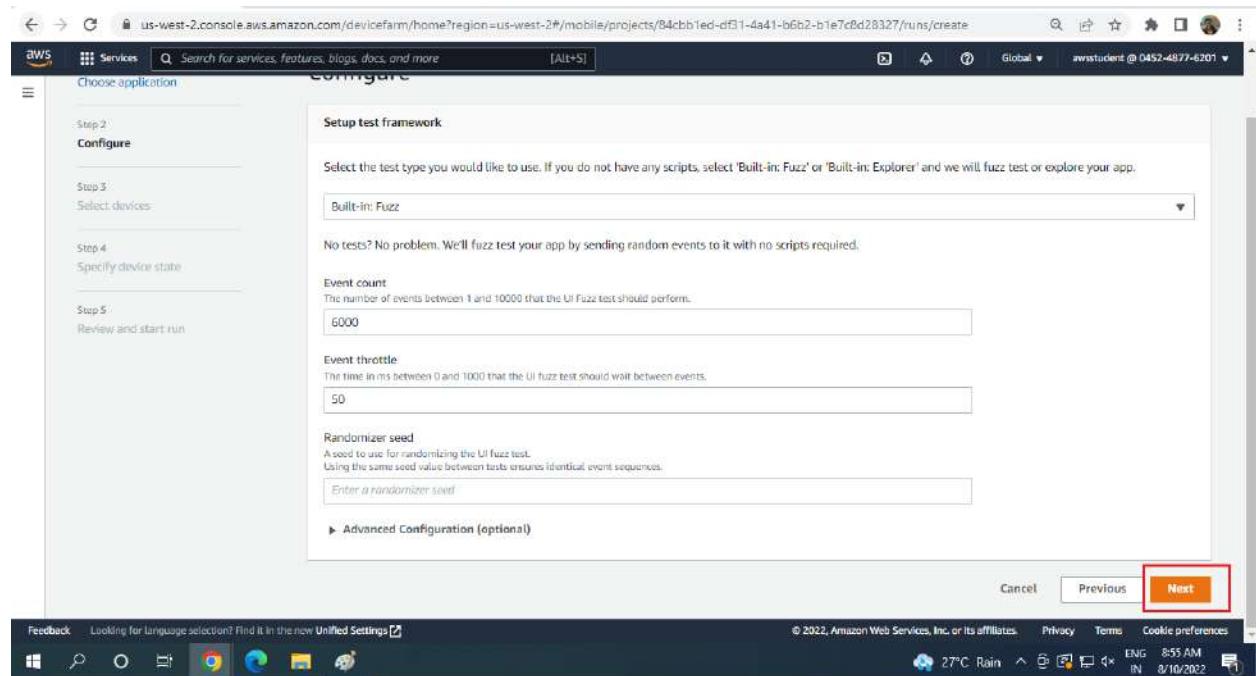
- Click Upload.
- Browse to and select the application that you downloaded.



Step 11 – Click Next.

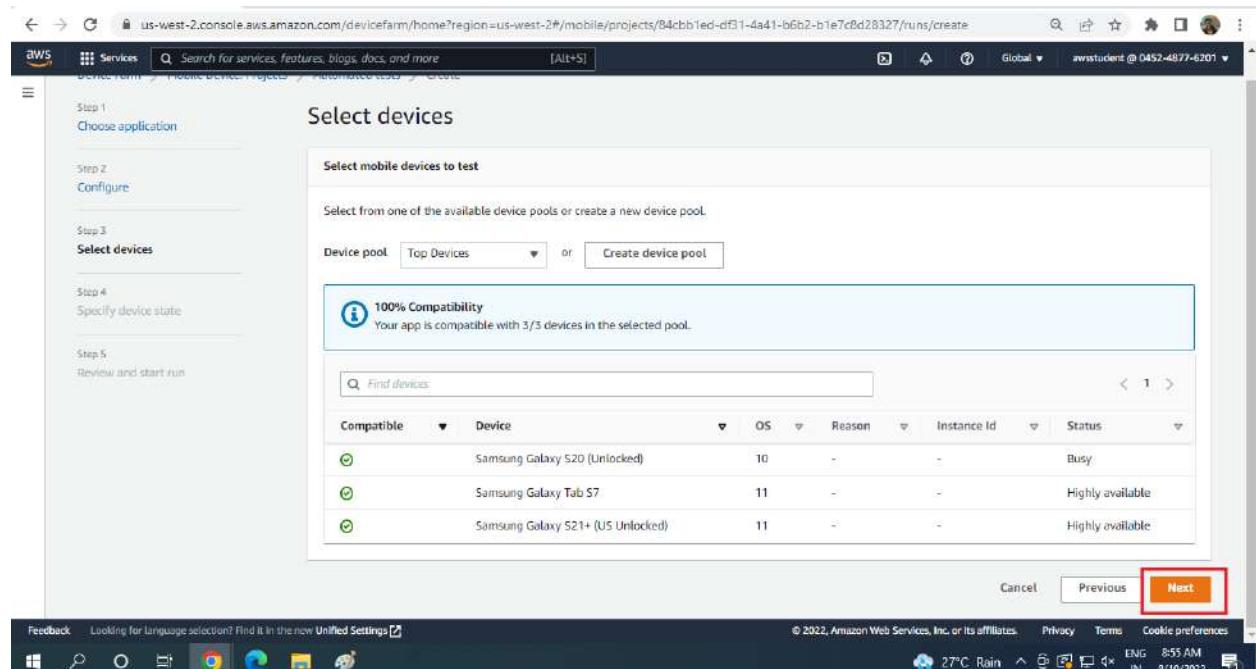


Step 12 – Click Next.



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

You will see the Top Devices pool.



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

Specify device state

Install additional software
Specify additional software to install on the mobile device.
Upload a .zip file to be extracted before your app is tested.
 or drop file here

Add extra data
Upload an .apk file as an extra data file. No instrumentation or provisioning required.
 or drop file here or

Location and network settings
Specify settings to simulate real-world scenarios and device configurations.

Set radio states

Device locale
Locales allow you to specify the language and region of the device:
English, US (en_US)

Network profile
Select a pre-defined Network profile or create a new one by clicking the button on the right:
Full

Device paths
Specify paths on the host machine and device where your files are stored separated by commas. These files will be available to view when the run is completed.

Host machine
Specify the comma separated paths where you want your files to be pulled from the host machine.
We recommend using the environment variable \$WORKING_DIRECTORY in your test code.
For allowed paths, refer to the documentation. Example: /tmp;SHOME:

Android
This root directory you can pull from is the application sandbox.
Pull files from Documents, Library, Media, and temp folders.
List file sharing enabled must be set to YES in your info.plist file in order to access device files.

Review and start run

Step 1 Choose application

Step 2 Configure

Step 3 Select devices

Step 4 Specify device state

Step 5 Review and start run

Run settings

Limit the maximum number of device minutes that your run can use by setting a timeout on each device. If execution exceeds your timeout, execution on that device will be forcibly stopped. Partial results will be available if possible.

You should choose a value that is greater than the anticipated duration of your tests. For example, if your tests take 20 minutes to complete you should choose a timeout of 30 minutes.

Set execution timeout

Maximum minutes per device. The timeout should be between 5 and 150:

150

Tags

No tags associated with the resource.

Add new tag

You can add up to 50 more tag(s).

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

Successfully created run "flickrj-android-sample-android.apk".

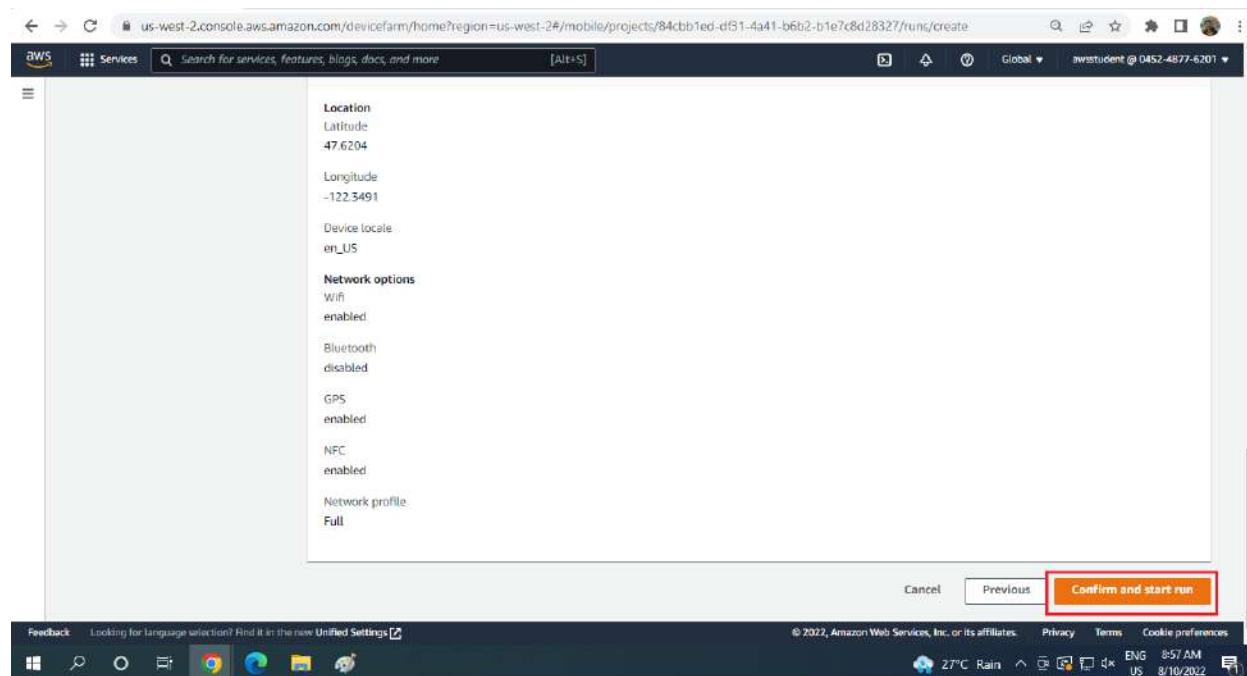
pavanProject

Project ARN: arn:aws:devicefarm:us-west-2:045248776201:project:84ccb1ed-df31-4a41-b6b2-b1e7c8d28327

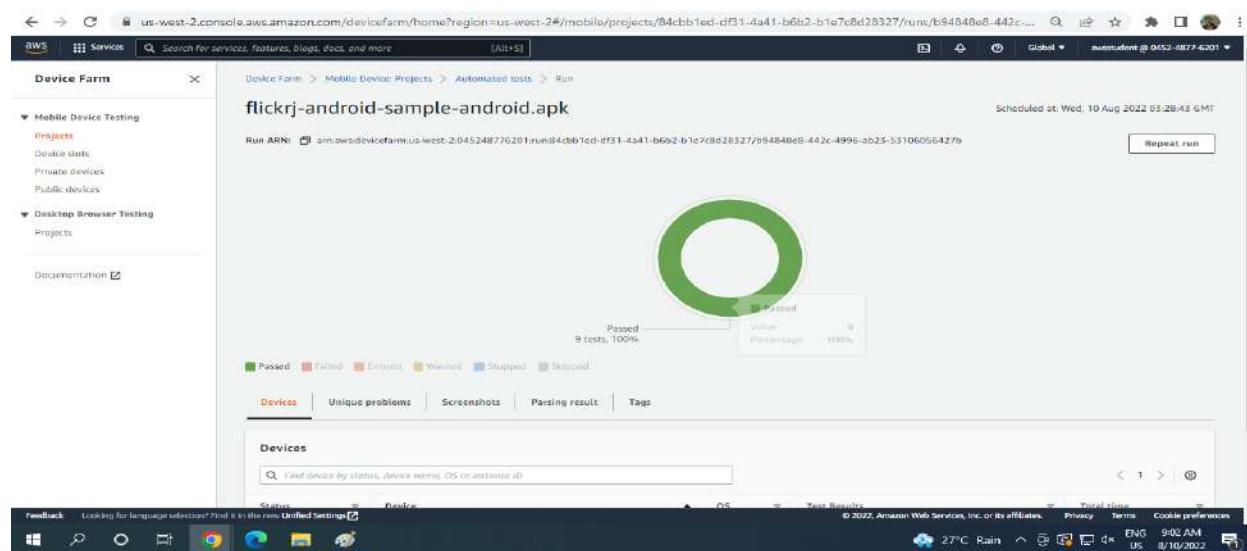
Automated tests

Create a new run

Status	Name	Test results	Test type	Created	Total time
Pending	flickrj-android-sample-android.apk	Passed: 0, errored: 0, failed: 0	Built-In: Fuzz	Wed, 10 Aug 2022 03:28:43 GMT	-



A summary page that includes the following information is displayed.



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

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

The screenshot shows the AWS Device Farm console interface. On the left, there's a sidebar with 'Mobile Device Testing' and 'Desktop Browser Testing' sections. The main area displays a green circular progress indicator with the text 'Passed' and '9 tests, 100%'. Below the progress indicator, there are tabs for 'Devices', 'Unique problems', 'Screenshots', 'Pining result', and 'Tags'. At the bottom, there's a 'Devices' section with a search bar and a table. The status bar at the bottom of the browser window shows the URL 'https://us-west-2.console.aws.amazon.com/devicefarm/logout?doLogout'.

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

The screenshot shows the 'Introduction to AWS Device Farm' lab page. On the left, there's a sidebar with 'Topics covered', 'Prerequisites', 'AWS Device Farm Introduction', 'AWS Device Farm Terminology', 'Start Lab', 'Task 1: Locate or Download an Example Application', 'Task 2: Upload and Test the Example Application', 'Task 3: Run Test and View the Run's Results', 'Conclusion', and 'End Lab'. The main area shows a timer at '00:21:54'. A red box highlights the 'End Lab' button. A modal dialog box is open, containing text about losing work if ending the lab and a 'Submit' button, which is also highlighted with a red box. The status bar at the bottom shows the URL '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=17289638'.

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

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

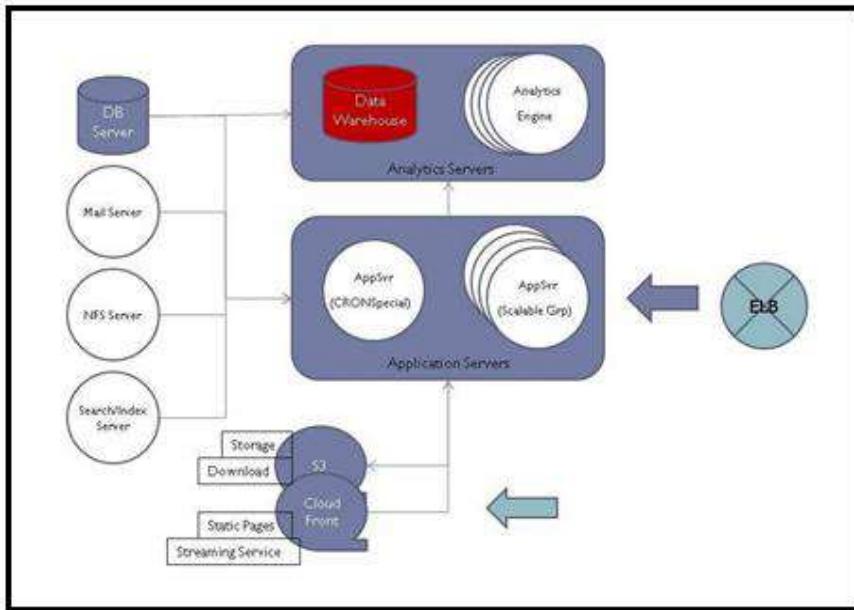
like Amazon Relational Database Service (Amazon RDS), Amazon CloudFront, Amazon CloudWatch, Elastic Load Balancing, and Amazon Route 53 confirm that the decision was the right one. As a startup, we have to worry about balancing scalability with cash preservation, and we get the best of both worlds with 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.

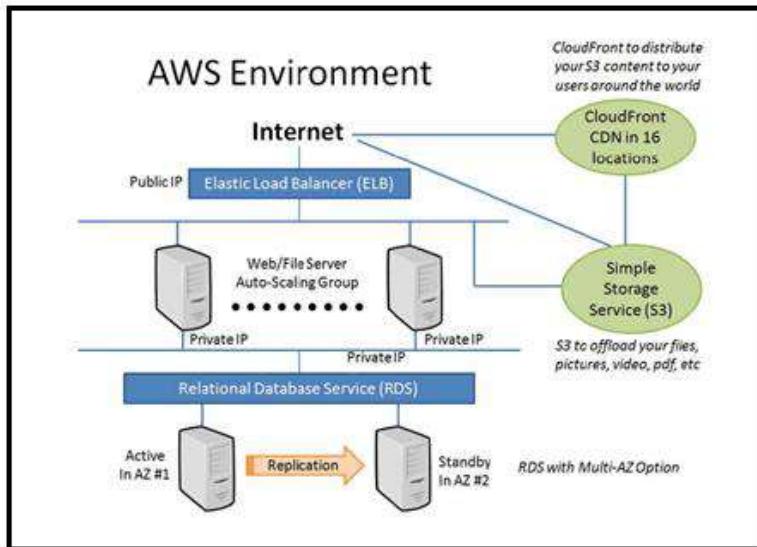
2. Before Cloud

- 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:

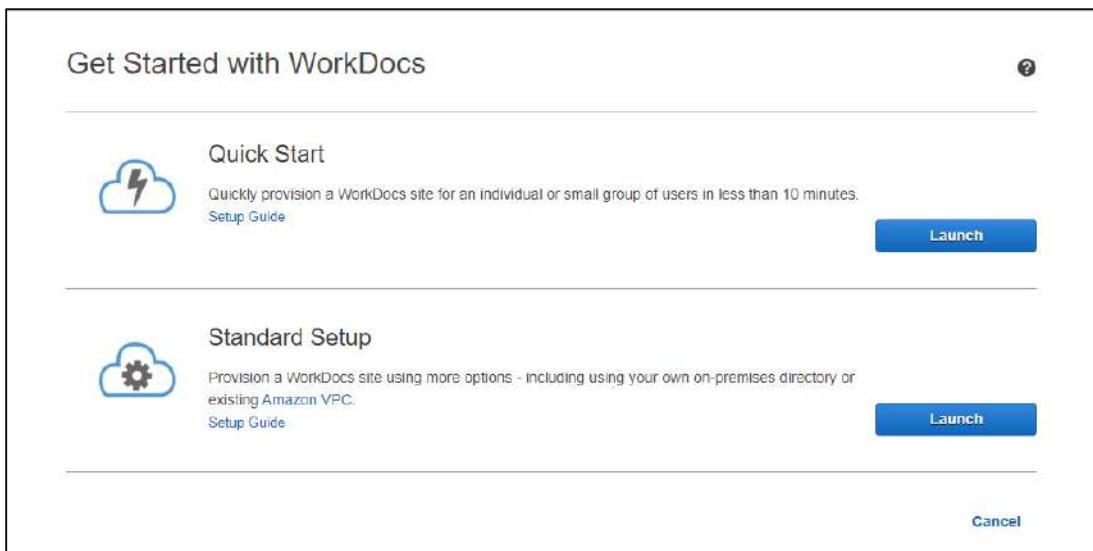
Step 1: Go to the particular link - <https://aws.amazon.com/workdocs/>



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.

WorkDocs Quick Start

Get up and running with Amazon WorkDocs immediately by filling in the fields below. Once you click "Complete Setup", Amazon will send an email invitation with instructions on how to quickly complete your profile. You will then be able to log in to your WorkDocs site, invite other users, and share documents.

Access Point

Region: Asia Pacific (Singapore) ?

Site URL: ?

Set WorkDocs Administrator

Email:

First Name:

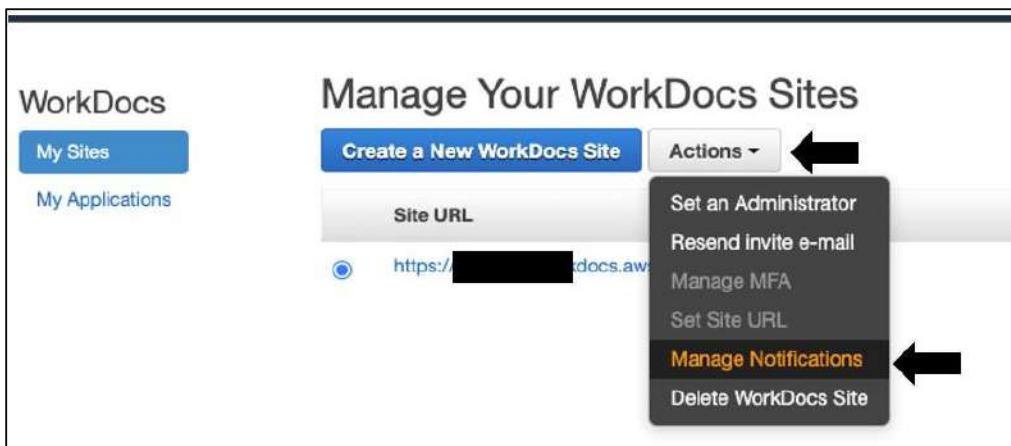
Last Name:

Cancel Complete Setup

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.

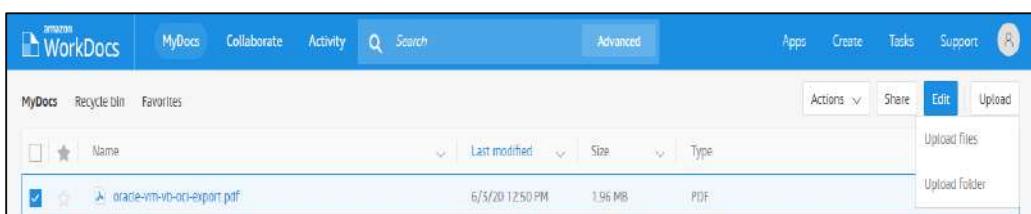
Step 8: If you didn't get an invite mail yet, select your created WorkDocs site, click Actions, and select Resend invite e-mail as shown in the following figure.



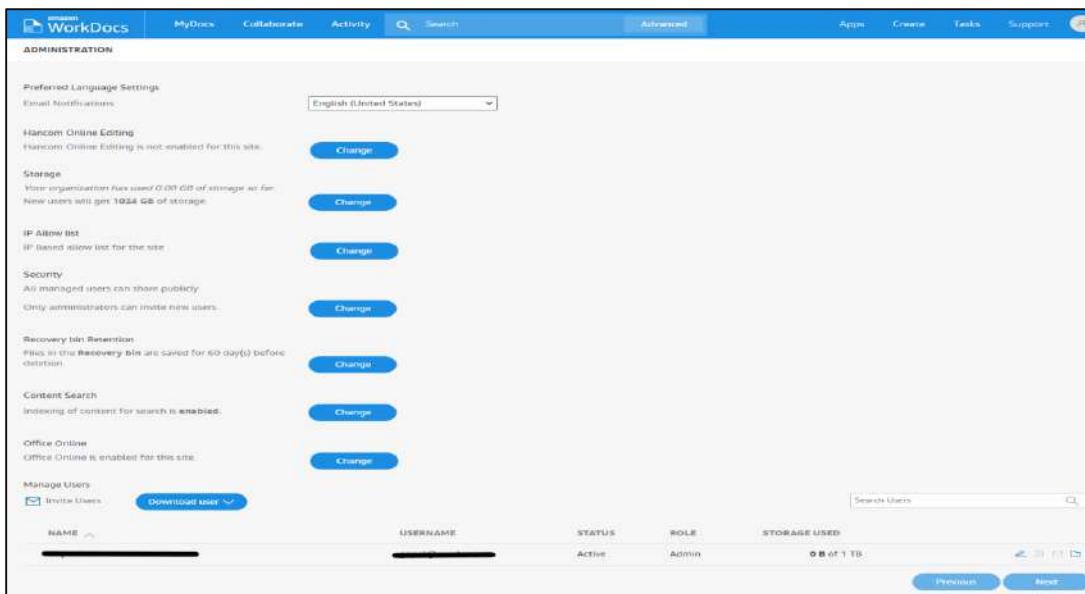
Step 9: Now, click your WorkDocs site link, type your registered email ID and login to WorkDocs console. You will see the WorkDocs console similar to as shown in the following figure.



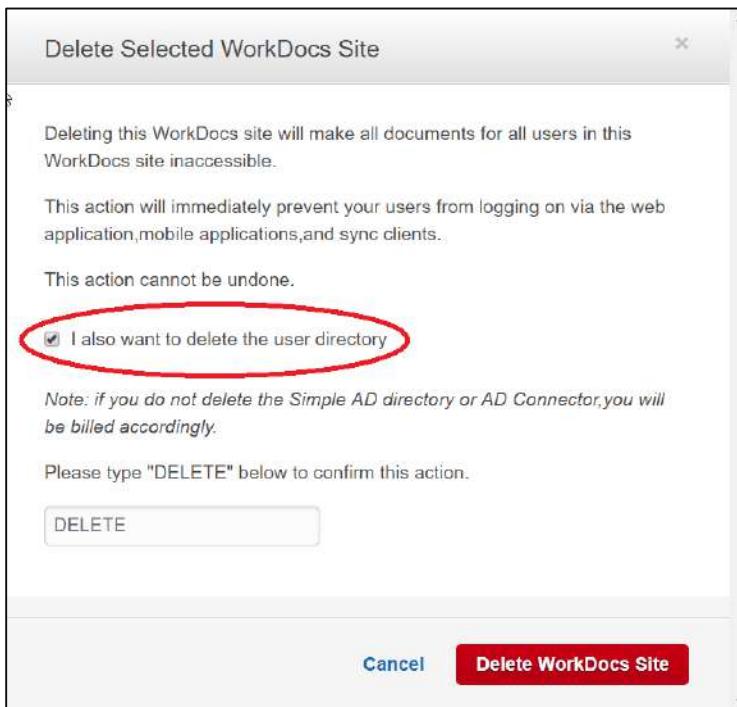
Step 10: In the right pane, you have various options to upload files and folders or create a new folder structure as shown in the following figure.



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 etc, 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 development 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.

The screenshot shows the AWS VPC Dashboard. On the left, there's a sidebar with options like 'New VPC Experience', 'VPC Dashboard', 'Subnets', 'Route Tables', 'Internet Gateways', etc. The main area displays 'Resources by Region' with counts for VPCs, Subnets, Route Tables, NAT Gateways, VPC Peering Connections, Network ACLs, Internet Gateways, Security Groups, and Customer Gateways. A 'Service Health' section indicates that 'Amazon EC2 - US East (N. Virginia)' is operating normally. On the right, there are sections for 'Settings' (Zones, Console Experiments), 'Additional Information' (VPC Documentation, All VPC Resources, Forums, Report an Issue), and a 'Transit Gateway Network Manager' link.

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

The screenshot shows the 'Step 1: Select a VPC Configuration' page. It lists three options: 'VPC with a Single Public Subnet' (selected), 'VPC with Public and Private Subnets', and 'VPC with a Private Subnet Only and Hardware VPN Access'. The 'VPC with a Single Public Subnet' section contains a description: 'Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.' Below this is a 'Creates:' section: 'A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.' To the right is a diagram showing a central 'Amazon Virtual Private Cloud' box connected to a 'Public Subnet' box, which in turn connects to 'Internet, S3, DynamoDB, SNS, SQS, etc.'. A blue 'Select' button is located at the bottom of this section.

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

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

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

- **IPv4 CIDR Block:** 10.50.0.0/16
- **VPC Name:** My_Test_VPC

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

Step 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:	<input type="text"/>	
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		
<input type="button" value="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

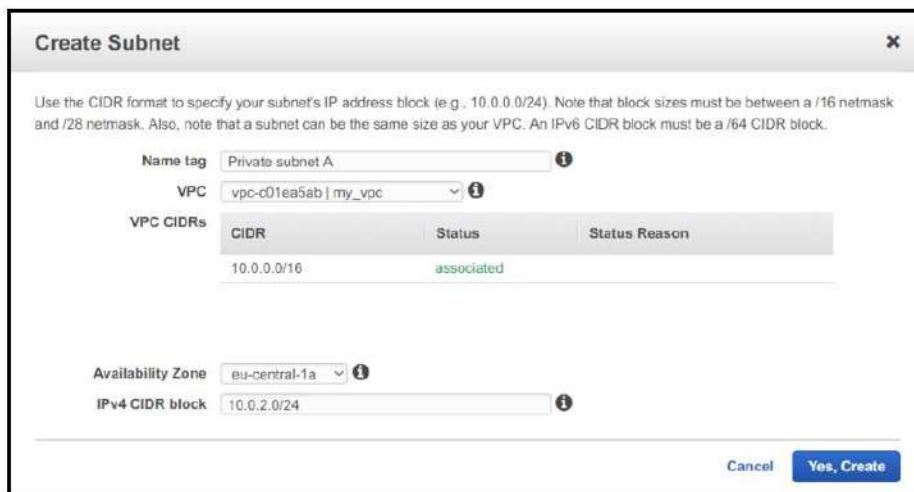
Step 1: Select the Subnets option in the navigation pane and then click Create Subnet.

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.

