



**RAMNIRANJAN JHUNJHUNWALA COLLEGE
GHATKOPAR (W), MUMBAI - 400 086**

**DEPARTMENT OF
INFORMATION TECHNOLOGY**

2021 - 2022

M.Sc. (I.T.) Part II (Sem - 3)

Subject: Amazon Web Services

**Name: Sneha Ramchandra Pawar.
Roll No.: 18**



Hindi Vidya Prachar Samiti's

**RAMNIRANJAN
JHUNJHUNWALA COLLEGE
(AUTONOMOUS)**

Opposite Ghatkopar Railway Station, Ghatkopar West, Mumbai-400086



CERTIFICATE

This is to certify that **Miss. Sneha Ramchandra Pawar** with Roll No. **18** has successfully completed the necessary course of experiments in the subject of **Amazon Web Services** during the academic year **2021 – 2022** complying with the requirements of **RAMNIRANJAN JHUNJHUNWALA COLLEGE OF ARTS, SCIENCE AND COMMERCE**, for the course of **M.Sc. (IT) Part II Semester – III.**

Internal Examiner

External Examiner

Head Of Department

College Seal

Index

Sr. No	Practical	Date	Page No.
1	Introduction		
A]	Creating AWS Free Tier Account		
B]	Getting Familiarised With The Aws Console		
2	An AWS IAM User https://amazon.qwiklabs.com/focuses/22172?catalog_rank=%7B%20rank%22%3A1%2C%22num_filters%22%3A0%2C%22has_search%20%3Atrue%7D&parent=catalog&search_id=14619834 https://amazon.qwiklabs.com/focuses/22172?parent=catalog		
A]	Explore users and groups		
B]	Add users to groups		
C]	Sign-In and test the users		
	Introduction to IAM Lab Steps Logging in to the Amazon Web Services Console Creating an IAM User Group Creating an IAM User Logging in using the new IAM credentials		
3	Working With S3 Buckets https://cloudacademy.com/lab/create-your-first-amazon-s3-bucket/ https://amazon.qwiklabs.com/focuses/22171?catalog_rank=%7B%20rank%22%3A1%2C%22num_filters%22%3A0%2C%22has_search%20%3Atrue%7D&parent=catalog&search_id=14619922		
A]	Create a bucket		

B]	Upload an object to the bucket		
C]	Make an object public		
D]	Create a bucket policy		
E]	Explore versioning		
	<p>Introduction to CloudWatch https://cloudacademy.com/lab/introduction-to-cloudwatch/</p> <p>Lab Steps</p> <p>Logging in to the Amazon Web Services Console</p> <p>Explore CloudWatch</p> <p>Monitoring EC2 Instances</p> <p>Install the EC2 Monitoring Scripts</p> <p>Creating Your First CloudWatch Alarm</p> <p>Create an Alarm using the EC2 console</p> <p>Sharing CloudWatch Metrics with others</p>		
4	<p>Introduction to Amazon API Gateway</p> <p>https://amazon.qwiklabs.com/focuses/10383?parent=catalog</p>		
A]	Create a Lambda Function		
B]	Test the Lambda function Conclusion		
5	<p>Introduction to Amazon DynamoDB</p> <p>https://amazon.qwiklabs.com/focuses/14815?catalog_rank=%7B%22rank%22%3A1%2C%22num_filters%22%3A0%2C%22has_search%22%3Atrue%7D&parent=catalog&search_id=14619942</p>		
A]	Create a new table		
B]	Add data		
C]	Modify existing items		
D]	Query the table		
E]	Delete the table		

6	<p>Introduction to Amazon Redshift</p> <p>https://amazon.qwiklabs.com/focuses/18468?catalog_rank=%7B%22rank%22%3A1%2C%22num_filters%22%3A0%2C%22has_search%22%3Atrue%7D&parent=catalog&search_id=14619952</p> <p>https://cloudacademy.com/lab/introduction-virtual-private-cloud-vpc/</p>		
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		
	Introduction to Virtual Private Cloud (VPC)		
	Lab Steps		
	Logging in to the Amazon Web Services Console		
	Creating a VPC		
	Creating a VPC subnet		
	Creating a VPC Internet Gateway		
	Connecting the Internet Gateway to the VPC Route Table		
	Creating an EC2 instance		
	Allocating and Associating an Elastic IP		
7	Introduction to AWS Key management Service		
	https://amazon.qwiklabs.com/focuses/22184?catalog_rank=%7B%22rank%22%3A1%2C%22num_filters%22%3A0%2C%22has_search%22%3Atrue%7D&parent=catalog&search_id=14619966		
	https://cloudacademy.com/lab/create-your-first-amazon-rds-database/		
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		
	Create Your First Amazon RDS Database Lab Steps Logging in to the Amazon Web Services Console Creating an RDS Subnet Group Setting up Security Group Rules for Connecting to the RDS Instance Creating a Database Using RDS Starting an AWS Systems Manager Session Manager Browser Shell Session Connecting to RDS and Creating a Database Table Deleting an RDS Database		
8	Case Study : Amazon Architecture		
	ABP News		
	Buzzdial		
	Classle		

Practical No. 1

Introduction

A) Creating AWS Free tier Account.

B) Getting Familiarised With The Aws Console

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

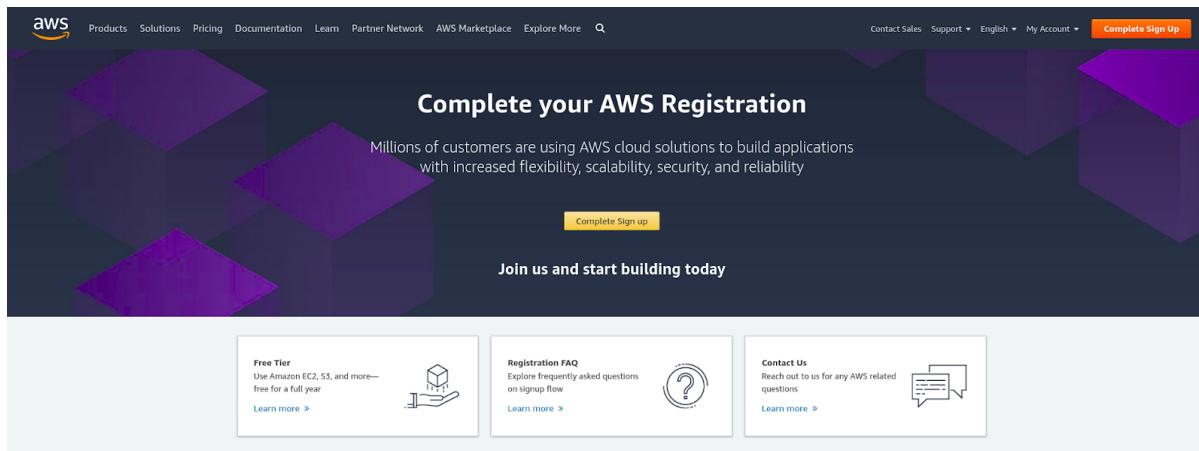
Creating an AWS Account is the first step you need to take in order to learn Amazon Web Services. Signing up for AWS provides you with all the tools you require to become an AWS professional.

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 Complete Sign Up button in the middle of the screen or on the top right corner of the screen. You will see the below screen.



Sign in ?

Email address of your AWS account

Or to sign in as an IAM user, enter your [account ID](#) or [account alias](#) instead.

Next

————— New to AWS? ————

Create a new AWS account



AWS Accounts Include 12 Months of Free Tier Access

Including use of Amazon EC2,
Amazon S3, and Amazon DynamoDB

Visit [aws.amazon.com/free](#) for full offer terms



About Amazon.com Sign In

Amazon Web Services uses information from your Amazon.com account to identify you and allow access to Amazon Web Services. Your use of this site is governed by our Terms of Use and Privacy Policy linked below. Your use of Amazon Web Services products and services is governed by the AWS Customer Agreement linked below unless you have entered into a separate agreement with Amazon Web Services or an AWS Value Added Reseller to purchase these products and services. The AWS Customer Agreement was updated on March 31, 2017. For more information about these updates, see [Recent Changes](#).

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Terms of Use](#) | [Privacy Policy](#) | [AWS Customer Agreement](#)

English ▾

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.

English ▾

Create an AWS account

AWS Accounts Include
12 Months of Free Tier Access

Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB
Visit [aws.amazon.com/free](#) for full offer terms

Email address

Password

Confirm password

AWS account name

Continue

[Sign in to an existing AWS account](#)

© 2019 Amazon Web Services, Inc. or its affiliates.
All rights reserved.
[Privacy Policy](#) · [Terms of Use](#)

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.

The screenshot shows the 'Contact Information' step of the AWS account creation process. At the top, it says 'Contact Information' and 'All fields are required.' Below that, instructions state: 'Please select the account type and complete the fields below with your contact details.' There are two radio buttons for 'Account type': 'Professional' (unchecked) and 'Personal' (checked). The 'Personal' option is selected. The form includes fields for 'Full name' (Saurabh Dashora), 'Phone number' (empty), 'Country/Region' (United States), 'Address' (Street, P.O. Box, Company Name, etc.), 'City' (empty), 'State / Province or region' (empty), and 'Postal code' (empty). A checkbox at the bottom left of the form area is checked, indicating agreement to the AWS Customer Agreement. At the bottom right, there is a yellow 'Create Account and Continue' button.

Note that unless you are creating an account for your organization, it is better to select Account Type as Personal.

After filling up the details, click on the Create Account and Continue button at the bottom of the form.

Step 3 – Filling up the Credit Card details

For Creating an AWS Account, you need to enter your Credit Card details.

The screenshot shows the 'Payment Information' step of the AWS account creation process. At the top, it says 'Payment Information'. Below that, instructions state: 'Please type your payment information so we can verify your identity. We will not charge you unless your usage exceeds the AWS Free Tier Limits. Review frequently asked questions for more information.' A note in a box explains: 'As part of our card verification process we will charge INR 2 on your card when you click the "Secure Submit" button below. This will be refunded once your card has been validated. Your bank may take 3-5 business days to show the refund. Mastercard/Visa customers may be redirected to your bank website to authorize the charge.' The form includes fields for 'Credit/Debit card number' (empty), 'Expiration date' (08 2019), and 'Cardholder's name' (empty).

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.

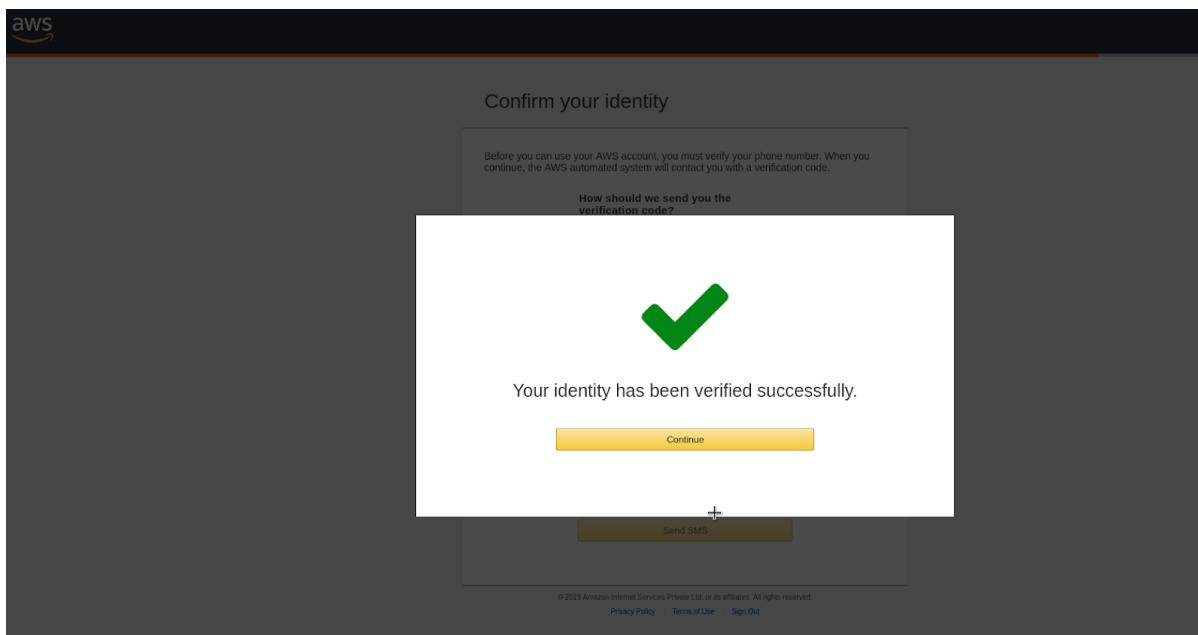
Step 4 – Identity Confirmation

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 'Confirm your identity' page. At the top, it says 'Before you can use your AWS account, you must verify your phone number. When you continue, the AWS automated system will contact you with a verification code.' Below this, there are two radio buttons for 'How should we send you the verification code?': 'Text message (SMS)' (selected) and 'Voice call'. A dropdown menu for 'Country or region code' is set to 'India (+91)'. A text input field for 'Cell Phone Number' is empty. Below these fields is a 'Security check' section containing a CAPTCHA image showing 'Y5785C' and a text input field where the user is expected to type the characters. A large yellow 'Send SMS+' button is at the bottom. At the very bottom of the page, there is small text: '© 2010 Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' followed by links to 'Privacy Policy', 'Terms of Use', and 'Sign Out'.

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.

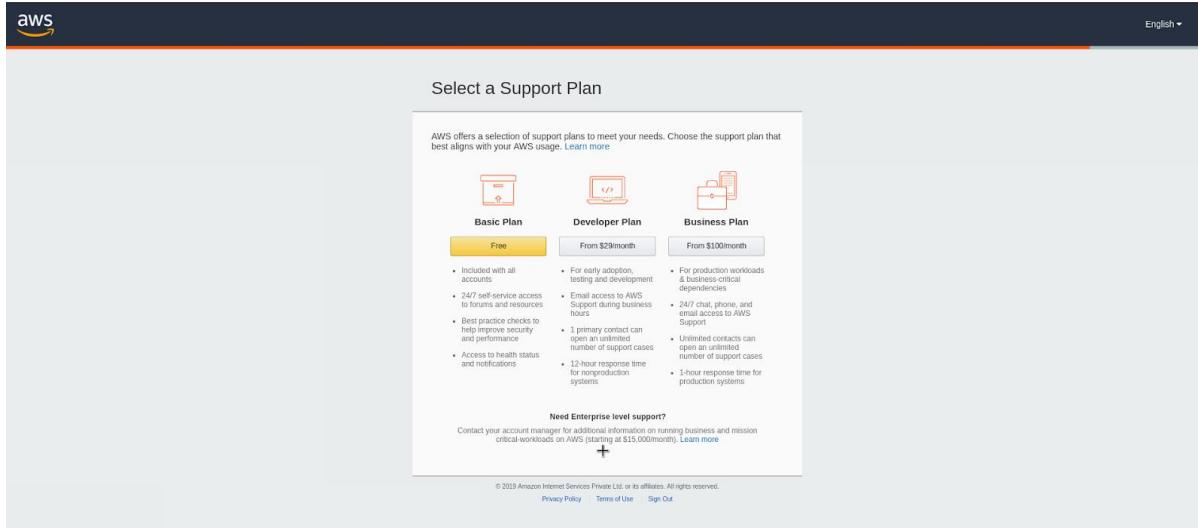
Once you have verified successfully, you should see a screen like below:



Click on Continue to proceed further.

Step 5 – Selecting a Support Plan

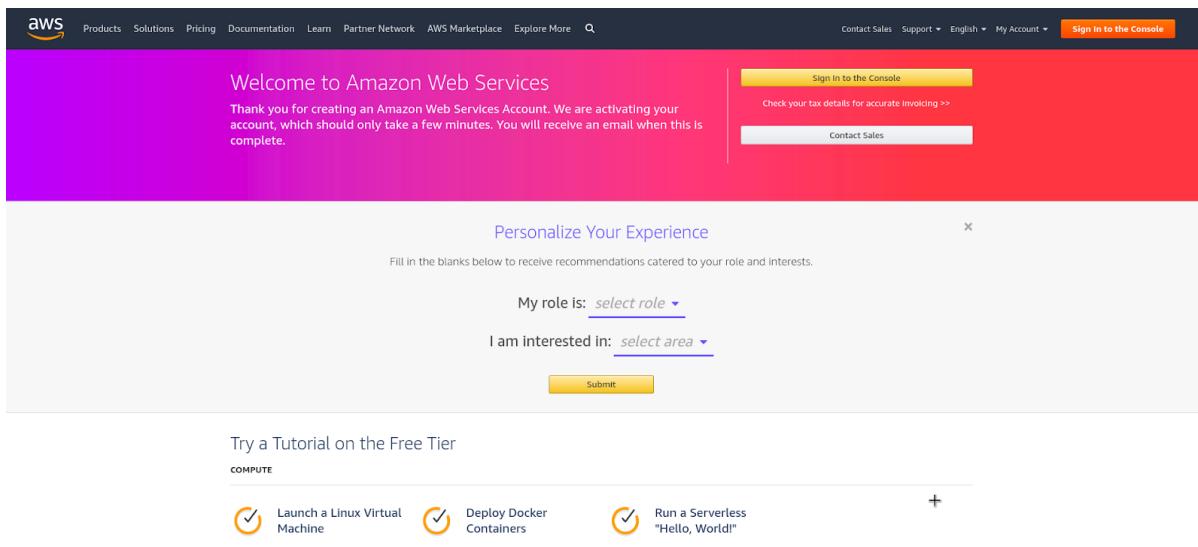
In the next step for creating an AWS Account, we need to select the plan for our AWS Account.



Unless you are planning to do some professional development, I would suggest selecting the Basic Plan. It is Free of cost and great for learning purposes.

The other plans are Developer Plan and a Business Plan. But both of them are paid options.

Once you select your plan, you will see the below Welcome screen. From here on, you can Sign in to your AWS Console.



Here, you also have the option of personalizing your experience of using Amazon Web Services.

However, you can also simply continue by clicking Sign in to the Console. After this, you will be again presented with the sign in screen where you can now use your credentials to login.

Finally, after logging in, you should be able to see the AWS Management Console as below:

The screenshot shows the AWS Management Console homepage. On the left, there's a search bar with placeholder text "Example: Relational Database Service, database, RDS". Below it is a "Find Services" section where you can enter names, keywords, or acronyms. A "All services" link is also present. In the center, there's a "Build a solution" section with several icons and descriptions: "Launch a virtual machine" (With EC2, 2-5 minutes), "Build a web app" (With Elastic Beanstalk, 6 minutes), "Build using virtual servers" (With Lightsail, 1-2 minutes), "Connect an IoT device" (With AWS IoT, 5 minutes); "Start a development project" (With CodeStar, 5 minutes), "Register a domain" (With Route 53, 3 minutes), "Deploy a serverless microservice" (With Lambda, API Gateway, 2 minutes), and "Create a backend for your mobile app" (With Mobile Hub, 5 minutes). To the right, there are sections for "Access resources on the go" (AWS Console Mobile App), "Explore AWS" (Amazon RDS, AWS Global Summits, AWS Marketplace, Open Distro for Elasticsearch), and "Find more services" (Search bar).

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](#).

The screenshot shows the AWS Free Tier page. At the top, there are three main categories: "Always free", "12 months free", and "Trials". Each category has a corresponding icon and a brief description. Below this, there's a "Free Tier details" section with a filter sidebar. The sidebar includes "Filter by:" dropdowns for "Tier Type" (with "Featured" checked) and "Product Categories" (with "Analytics" checked). The main area displays three service offerings: "Amazon EC2" (750 Hours per month, Free Tier, 12 MONTHS FREE), "Amazon S3" (5 GB of standard storage, Free Tier, 12 MONTHS FREE), and "Amazon RDS" (750 Hours per month of db.t2.micro database usage (MySQL, PostgreSQL, MariaDB), Free Tier, 12 MONTHS FREE).

In our series of learning AWS, we will try to keep ourselves within the free tier as much as possible.

Conclusion

We have now successfully finished creating an AWS Account and also verified it so that it can be used to learn AWS.

B]

Getting Familiarized with the AWS Console :

The screenshot shows the AWS Management Console interface for the Amazon EC2 service. A red arrow points to the top navigation bar, which includes links for Elastic Beanstalk, S3, EC2, VPC, CloudWatch, Elastic MapReduce, CloudFront, CloudFormation, RDS, ElastiCache, SQS, IAM, SNS, and SES. Another red arrow points to the left Navigation Pane, which lists various services: EC2 Dashboard, INSTANCES (with sub-options like Instances, Spot Requests, Reserved Instances), IMAGES (AMIs, Bundle Tasks), ELASTIC BLOCK STORE (Volumes, Snapshots), and NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups, Load Balancers, Key Pairs). A third red arrow points to the 'Current page', which is 'Instances' under the 'INSTANCES' section. The main content area is titled 'My Instances' and displays a table with one row for an EC2 instance named 'empty'. The table columns are Name, Instance, AMI ID, Root Device, Type, Status, and Security Groups. Below the table, a message says '1 EC2 Instance selected.' followed by the instance details: EC2 Instance: i-ab059cc8 ec2-50-17-14-16.compute-1.amazonaws.com. A detailed view of the instance is shown in a modal window, with the 'Public DNS' field ('ec2-50-17-14-16.compute-1.amazonaws.com') highlighted with a red box.

Navigation bar : Navigation bar provides a unified search tool for tracking down AWS services and features, service documentation, and AWS Marketplace.

Navigation Pane : The main dashboard is selected by default on the homepage of the AWS console, One can navigate to any pages using navigation pane.

Current Page : Current Page is the page to which we navigate through Navigation Pane. In the current scenario the current page is of EC2 Instances

Public DNS : Public DNS — **The external DNS hostname**. When you launch an EC2 instance, it is assigned a public IP address and a public DNS (Domain Name System) name that you can use to reach it from the internet. Because there are so many hosts in the Amazon Web Services domain, these public names must be quite long for each name to remain unique.

Private DNS : Private IPv4 addresses enable communication within the network of the instance. You can use the Route 53 Private DNS feature to manage **authoritative** DNS within your Virtual Private Clouds (VPCs), so you can use custom domain names for your internal AWS resources without exposing DNS data to the public Internet.

Zone : An Availability Zone (AZ) is **one or more discrete data centers with redundant power, networking, and connectivity** in an AWS Region.

The screenshot shows the AWS EC2 Management Console interface. The navigation bar at the top includes links for AWS, Services, Resource Groups, and a user profile. The region selector dropdown is set to "Oregon". The navigation pane on the left is highlighted with a red box and contains sections for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, Elastic Block Store, Network & Security, and Auto Scaling. The "Instances" tab is highlighted with a green box. The main content area displays a table of EC2 instances with columns for Name, Instance ID, Instance Type, Availability Zone, Instance State, and Status Checks. One instance, i-baad0ab2, is selected and its details are shown in a modal-like overlay at the bottom. The details include Instance ID (i-baad0ab2), Instance state (stopped), Instance type (m1.small), Private DNS (-), Private IPs (-), Secondary private IPs (-), VPC ID (-), Public DNS (-), Public IP (-), Elastic IP (-), Availability zone (us-west-2b), Security groups (test-WebServerSecurityGroup-1KLAPZBYEK4E3, view rules), and Scheduled events (-). The bottom of the screen shows standard AWS footer links for Feedback, English, Privacy Policy, and Terms of Use.

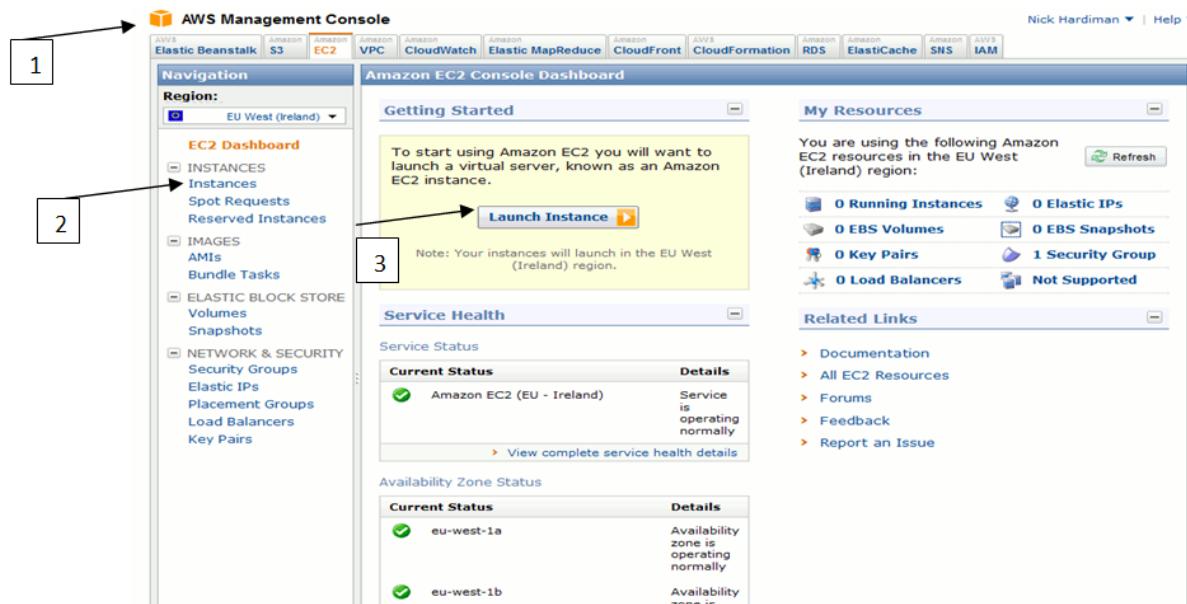
Description of :

Instance ID : Amazon Connect instance ID is **the 36-character string at the end of your instance's Amazon Resource Name (ARN)**.

Instance State : Instance state shows the status of the Instance whether it is running or stopped.

Instance Type: Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications. Each instance type includes one or more instance sizes, allowing you to scale your resources to the requirements of your target workload.

Security Groups: A security group **acts as a virtual firewall for your EC2 instances to control incoming and outgoing traffic**.



Description :

1. AWS console is **the web application that allows users to access Amazon web services**. Without the console presented in a way users can easily navigate to every Amazon web service, it will be difficult to have centralized access to all the Amazon web services.
2. An instance is **a virtual server in the AWS Cloud**. With Amazon EC2, you can set up and configure the operating system and applications that run on your instance. When you sign up for AWS, you can get started with Amazon EC2 using the AWS Free Tier.
3. Launch instances are **virtual machines that run inside the cloud**. Before you can launch an instance, gather the following parameters: The instance source can be an image, snapshot, or block storage volume that contains an image or snapshot. A name for your instance.

Practical No. 2

An AWS IAM User

Aim: A) Explore users and groups

- B) Add users to groups
- C) Sign-In and test the users
- D) Introduction to IAM

Lab Steps

Logging in to the Amazon Web Services Console

Creating an IAM User Group

Creating an IAM User

Logging in using the new IAM credentials

A) Explore users and groups

In AWS console -> services menu ->click IAM

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and user information. Below the search bar is a sidebar titled "AWS services" which includes "Recently visited services" (CloudWatch, Systems Manager, EC2, IAM) and a "All services" link. In the main content area, there's a section titled "Stay connected to your AWS resources on-the-go" featuring the AWS Console Mobile App. To the right of this is another section titled "Explore AWS" and "Free AWS Training". At the bottom of the screen, there's a dark footer bar with various icons and links.

In the navigation pane -> click on users

The screenshot shows the AWS Identity and Access Management (IAM) service. In the top navigation bar, there is a search bar with placeholder text "Search for services, features, blogs, docs, and more". Below the search bar, a blue banner displays the message: "Introducing the new Users list experience. We've redesigned the Users list experience to make it easier to use. [Let us know what you think.](#)". The main content area is titled "Users (5) Info" and contains a table with the following data:

User name	Groups	Last activity	MFA	Password a..
awsstudent	QLReadOnly	None	None	5 minutes ago
root-qwkl	None	None	None	None
user-1	None	None	None	4 minutes ago
user-2	None	None	None	4 minutes ago
user-3	None	None	None	4 minutes ago

On the right side of the table, there are buttons for "Delete" and "Add users". The left sidebar contains navigation links for "Identity and Access Management (IAM)", "Dashboard", "Access management", "User groups", "Users" (which is selected), "Roles", "Policies", "Identity providers", "Account settings", "Access reports", "Access analyzer", "Archive rules", "Analyzers", and "Settings". At the bottom of the page, there is a footer with copyright information and links for "Feedback", "English (US)", "Privacy", "Terms", and "Cookie preferences".

Click on user 1 this will bring you on summary page with permission tab

The screenshot shows the "Summary" page for the user "user-1". The top navigation bar includes a back arrow, the text "Users > user-1", and buttons for "Delete user" and "Edit user". The main content area is titled "Summary" and displays the following details:

User ARN	arn:aws:iam::497177492769:user/spl66/user-1
Path	/spl66/
Creation time	2021-11-25 14:06 UTC+0530

Below these details, there is a navigation bar with tabs: "Permissions" (selected), "Groups", "Tags (2)", "Security credentials", and "Access Advisor". The "Permissions" tab is currently active, showing a section titled "Permissions policies" with the following content:

i 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](#)

Buttons for "Add permissions" and "Add inline policy" are present at the bottom of this section.

The footer of the page includes standard AWS footer links: "© 2021, Amazon Web Services, Inc. or its affiliates.", "Privacy", "Terms", "Cookie preferences", and icons for "34°C Smoke", "ENG IN", "14:14", and "25-11-2021".

Notice that user-1 does not have any permissions.

7. 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 'Groups' tab is selected, indicating that the user is not a member of any groups. The page includes details such as User ARN, Path, and Creation time. A prominent blue button labeled 'Add user to groups' is visible. The bottom of the screen shows a dark footer bar with various system icons and status information.

Users > user-1

Summary

User ARN: arn:aws:iam::497177492769:user/spl66/user-1 [Edit](#)

Path: /spl66/

Creation time: 2021-11-25 14:06 UTC+0530

Permissions Groups Tags (2) Security credentials Access Advisor

Add user to groups

Group name	Attached permissions
	No results

© 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

34°C Smoke ENG 14:19 IN 25-11-2021 1

8. Click the Security credentials tab.

user-1 is assigned a Console password

User ARN arn:aws:iam::497177492769:user/spl66/user-1 [Edit](#)

Path /spl66/

Creation time 2021-11-25 14:06 UTC+0530

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

Sign-in credentials

Summary • Console sign-in link: <https://497177492769.signin.aws.amazon.com/console> [Edit](#)

Console password Enabled (never signed in) | [Manage](#)

Assigned MFA device Not assigned | [Manage](#)

Signing certificates None [Edit](#)

Access keys

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

© 2021, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

34°C Smoke ENG IN 14:20 25-11-2021 [Feedback](#)

9. In the navigation pane on the left, click User Groups.

The following groups have already been created for you:

EC2-Admin

- EC2-Support
- S3-Support

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, there's a sidebar with options like Dashboard, User groups, Roles, Policies, Identity providers, Account settings, and more. The main area is titled "User groups (4)" and contains a table with columns: Group name, Users, Permissions, and Creation time. The table shows the following data:

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	13 minutes ago
EC2-Support	0	Defined	13 minutes ago
QLReadOnly	1	Defined	13 minutes ago
S3-Support	0	Defined	13 minutes ago

At the bottom of the page, there are links for Feedback, English (US), and various system status indicators.

10. Click the EC2-Support group.

This screenshot shows the summary page for the "EC2-Support" user group. The top navigation bar includes links for IAM, User groups, and EC2-Support. The main title is "EC2-Support". Below it is a "Summary" section with tabs for Edit, User group name (EC2-Support), Creation time (November 25, 2021, 14:06 (UTC+05:30)), and ARN (arn:aws:iam::497177492769:group/spl6/EC2-Support). There are three tabs at the bottom: "Users" (selected), "Permissions", and "Access Advisor".

Users in this group (0)

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

Search bar: Search

Bottom navigation bar: © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences. System status: 34°C Smoke. Date and time: 25-11-2021 14:23.

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

11. Click the Permissions tab.

The screenshot shows the AWS IAM Groups page. At the top, there's a summary section with details: User group name (EC2-Support), Creation time (November 25, 2021, 14:06 (UTC+05:30)), and ARN (arn:aws:iam::497177492769:group/spl6/EC2-Support). Below this, there are tabs for 'Users', 'Permissions' (which is selected), and 'Access Advisor'. Under the 'Permissions' tab, there's a section for 'Permissions policies (1) Info'. It says 'You can attach up to 10 managed policies.' and includes buttons for 'Simulate' and 'Remove', and a dropdown for 'Add permissions'. A search bar and navigation controls are also present. A table lists the single policy: 'AmazonEC2ReadOnlyAccess' (AWS managed, Type). The bottom of the screen shows the AWS footer with copyright information, privacy terms, cookie preferences, and various status icons.

This group has a Managed Policy associated with it, called

AmazonEC2ReadOnly Access 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

12. Click on Amazon EC2ReadOnly Access under Permissions tab and a new browser window opens. Now click on () JSON.

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, Elastic Load Balancing, CloudWatch and Auto Scaling. This ability to view resources, but not modify them, is ideal for assigning to a Support

Summary

Policy ARN arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess 

Description Provides read only access to Amazon EC2 via the AWS Management Console.

Permissions Policy usage Policy versions Access Advisor

Policy summary  

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": "ec2:Describe*",  
7       "Resource": "*"  
8     },  
9   ]
```

read-only 

© 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
34°C Smoke ENG 14:24
IN 25-11-2021 

In the navigation pane on the left, click User Groups

14 Click the S3-Support group.

The S3-Support group has the Amazon S3ReadOnlyAccess policy attached

Summary

User group name: S3-Support | Creation time: November 25, 2021, 14:06 (UTC+05:30) | ARN: arn:aws:iam::497177492769:group/spl66/S3-Support

Permissions

Permissions policies (1) Info

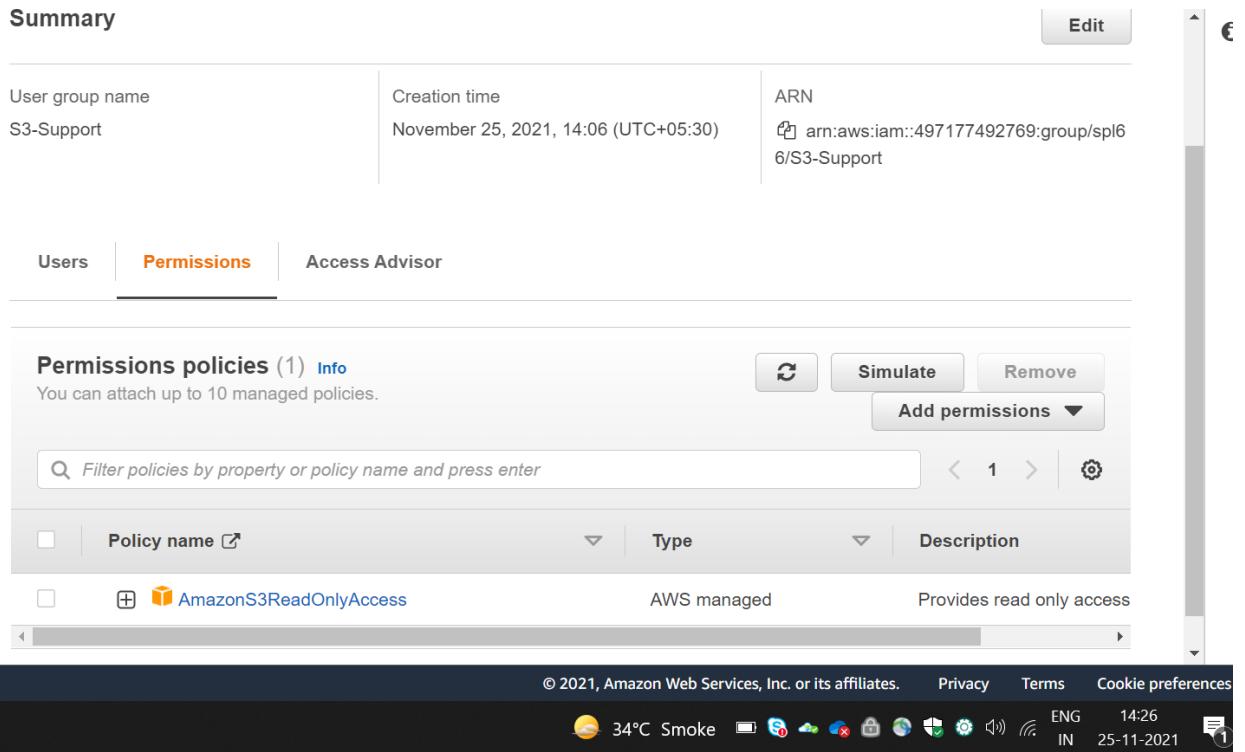
You can attach up to 10 managed policies.

Add permissions

Filter policies by property or policy name and press enter

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	Provides read only access

© 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
34°C Smoke ENG 14:26 IN 25-11-2021



15. Click on Amazon S3ReadOnly Access under Permissions tab and a new browser window opens. Now click on () JSON.

This policy has permissions to Get and List resources in Amazon \$3.

Policies > AmazonS3ReadOnlyAccess

Summary

Policy ARN arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess [?](#)

Description Provides read only access to all buckets via the AWS Management Console.

Permissions **Policy usage** **Policy versions** **Access Advisor**

Policy summary [{ } JSON](#)

```
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      ]
11    }
12  ]
13}
```

read-only [?](#)

© 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

34°C Smoke 📱 ENG 14:27 IN 25-11-2021

16. In the navigation pane on the left, click User Groups

17. Click the EC2-Admin group.

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

Summary

User group name: EC2-Admin

Creation time: November 25, 2021, 14:06 (UTC+05:30)

ARN: arn:aws:iam::497177492769:group/spl6/EC2-Admin

Permissions

Permissions policies (1) [Info](#)

You can attach up to 10 managed policies.

Add permissions

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	EC2-Admin-Policy	Customer inline	

© 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
34°C Smoke ENG 14:28 IN 25-11-2021

click on EC2 admin policy Access under Permissions tab and a new browser window opens. Now click on () JSON.

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor **JSON** **Import managed policy**

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": [
6         "ec2:Describe*",
7         "ec2:StartInstances",
8         "ec2:StopInstances",
9         "cloudwatch:DescribeAlarms"
      ]
    }
  ]
}

```

Character count: 170 of 5,120.
The current character count includes character for all inline policies in the group: EC2-Admin.

Cancel **Review policy**

B) Add users to groups

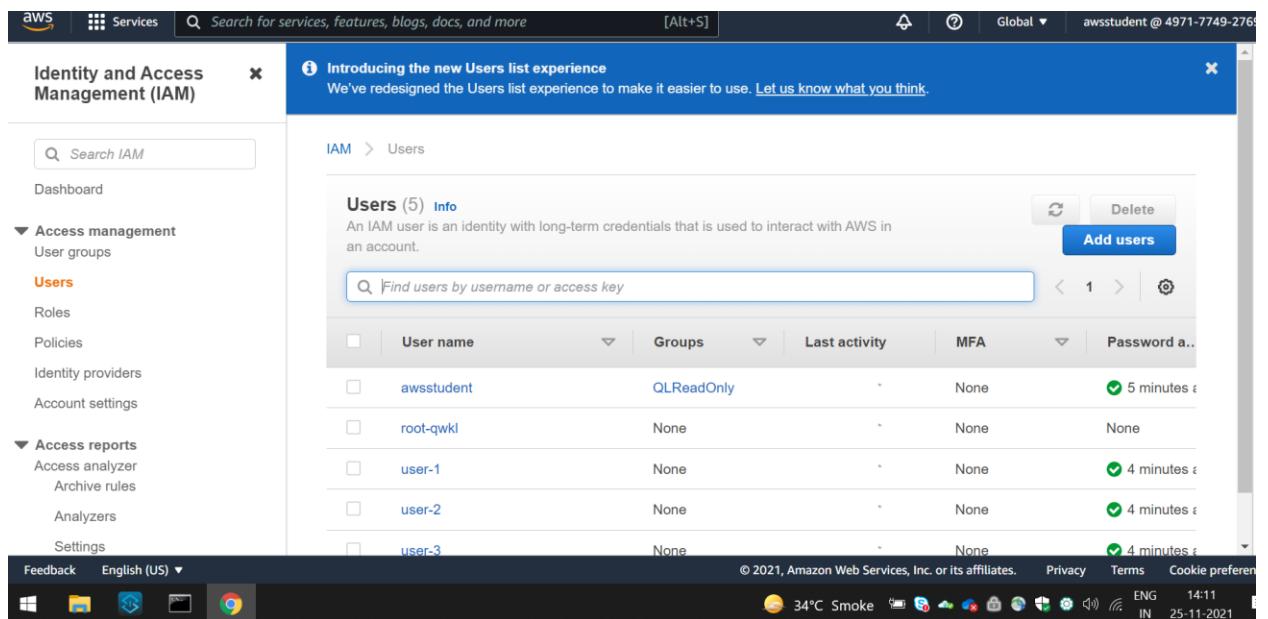
Add user-1 to the S3-Support Group

20. In the left navigation pane, click User Groups

21. Click the S3-Support group.

22. Click the Users tab.

23. In the Users tab, click Add Users to Group



The screenshot shows the AWS Identity and Access Management (IAM) service interface. The left sidebar has 'Identity and Access Management (IAM)' selected. The main area shows a table of users:

User Name	Groups	Last Activity	MFA	Created
awsstudent	QLReadOnly	None	None	5 minutes ago
root-qwkl	None	None	None	None
user-1	None	None	None	4 minutes ago
user-2	None	None	None	4 minutes ago
user-3	None	None	None	4 minutes ago

A blue callout box at the top right of the table says: "Introducing the new Users list experience. We've redesigned the Users list experience to make it easier to use. Let us know what you think." There is a "Add users" button in the top right corner of the table area.

In the Add Users to Group window, configure the following

Select user-1.

At the bottom of the screen, click Add Users

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

The screenshot shows the 'Add users to S3-Support' dialog. At the top, it says 'Other users in this account (Selected 1/5)'. Below is a table with columns: User name, Groups, Last activity, and Creation time. The table lists four users:

User name	Groups	Last activity	Creation time
awsstudent	1	None	2 years ago
root-qwkl	You need permissions	None	2 years ago
<input checked="" type="checkbox"/> user-1	0	None	24 minutes ago
<input type="checkbox"/> user-2	0	None	24 minutes ago
<input type="checkbox"/> user-3	0	None	24 minutes ago

At the bottom right, there are 'Cancel' and 'Add users' buttons. The 'Add users' button is highlighted in blue. The footer includes links for 'Privacy', 'Terms', and 'Cookie preferences'.

Add user-2 to Ec2 support by same steps

Add users to EC2-Support

Other users in this account (Selected 1/5) [Info](#)

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	awsstudent	1	None	2 years ago
<input type="checkbox"/>	root-qwkl		You need permissions	None 2 years ago
<input type="checkbox"/>	user-1	1	None	31 minutes ago
<input checked="" type="checkbox"/>	user-2	0	None	31 minutes ago
<input type="checkbox"/>	user-3	0	None	31 minutes ago

[Cancel](#) [Add users](#)

© 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
34°C Smoke ENG IN 25-11-2021

Add user-3 to Ec2 admin

Add users to EC2-Admin

Other users in this account (Selected 1/5) [Info](#)

<input type="checkbox"/>	User name	Groups	Last activity	Creation time
<input type="checkbox"/>	awsstudent	1	None	2 years ago
<input type="checkbox"/>	root-qwkl		You need permissions	None 2 years ago
<input type="checkbox"/>	user-1	1	None	32 minutes ago
<input type="checkbox"/>	user-2	0	None	32 minutes ago
<input checked="" type="checkbox"/>	user-3	0	None	32 minutes ago

[Cancel](#) [Add users](#)

© 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
34°C Smoke ENG IN 25-11-2021

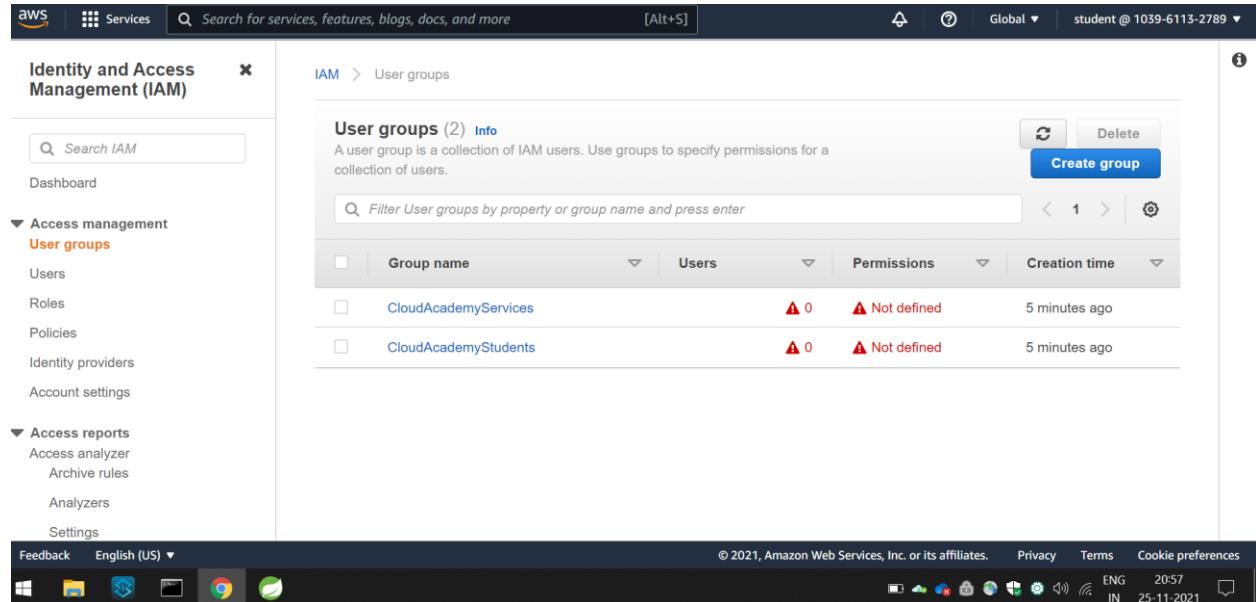
Sign-In and test the users

Creating an IAM User Group

In the AWS Management Console search bar, enter **IAM**, and click the **IAM** result under **Services**:

From the IAM dashboard, click on **User groups** link in the sidebar menu:

You will see errors indicating your student user does not have permissions to perform specific actions:



The screenshot shows the AWS IAM User Groups page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' selected. The main area shows 'User groups (2)'. There are two entries in the table:

Group name	Users	Permissions	Creation time
CloudAcademyServices	⚠ 0	⚠ Not defined	5 minutes ago
CloudAcademyStudents	⚠ 0	⚠ Not defined	5 minutes ago

A blue 'Create group' button is located at the top right of the table area. The bottom of the screen shows the AWS footer with various icons and links.

Click on the **Create Group** blue button for creating a new IAM group:

In the **User group name** field, enter **DevOps** as the name of the group:



Create user group

Name the group

User group name

Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+,-,@-_ ' characters.

Add users to the group - *Optional* (2) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.



<

1

>



© 2021, Amazon Web Services, Inc. or its affiliates.

[Privacy](#)
[Terms](#)
[Cookie preferences](#)


ENG

20:58
IN

Skip down to the **Attach permissions policies** section, enter *AmazonEC2ReadOnlyAccess* into the search bar and select the resulting policy: **AmazonEC2ReadOnlyAccess**:

Attach permissions policies - *Optional*
(Selected 1/714)

Info
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

1 match < 1 >

Properties	X	"AmazonEC2ReadOnlyAccess" X	Clear filters
Type	name ↗	Type	Description
Path		AWS managed	Provides read only
Used as	AmazonEC2ReadOnlyAccess		

Create group

Click **Create Group**.

The **Groups** page now lists the new group and you are able to assign the DevOps group to any available user:

The screenshot shows the AWS IAM User Groups page. At the top, a green banner displays the message "DevOps user group created." with a checkmark icon. Below the banner, the navigation path is "IAM > User groups". The main title is "User groups (3) Info". A sub-instruction says "A user group is a collection of IAM users. Use groups to specify permissions for a collection of users." On the right, there are "View group", "Delete", and "Create group" buttons. A search bar is labeled "Filter User groups by property or group name and press enter". Below the search bar are buttons for "Reset" and "Delete". The table has columns: "Group name", "Users", "Permissions", and "Creation time". The table contains three rows: "CloudAcademyServices" (Permissions: Not defined, Creation time: 11 minutes ago), "CloudAcademyStudents" (Permissions: Not defined, Creation time: 11 minutes ago), and "DevOps" (Permissions: Defined, Creation time: Now). The bottom of the page includes a footer with copyright information, privacy terms, cookie preferences, and system status icons.

Creating an IAM User

click on **Users** in the sidebar menu:

Click **Add user** to begin creating a new user:

Enter the following values in the form:

- **User name:** John (Name must be case sensitive)
- **Access key - Programmatic access:** Checked
- **Password - AWS Management Console access:** Checked

- **Console password: Autogenerated password**
- **Require password reset:** Unchecked

Add user

1 2 3 4 5

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Select AWS credential type* **Access key - Programmatic access**
 Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- Password - AWS Management Console access**
 Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* Autogenerated password
 Custom password

Require password reset User must create a new password at next sign-in

* Required

[Cancel](#)

[Next: Permissions](#)

Click **Next: Permission** to advance to the next step.

Click **Next: Tags**. Skip this page and click on **Next: Review**.

You will add the user to the DevOps Group later.

Add user

1 2 3 4 5

Set permissions



Add user to group



Copy permissions from
existing user



Attach existing policies
directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Add user to group

[Create group](#)

Refresh

Search

Showing 3 results

Group ▾

Attached policies

[Cancel](#)

[Previous](#)

[Next: Tags](#)

Add user

1 2 3 4 5

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Add new key"/>	<input type="text"/>	Remove

You can add 50 more tags.

[Cancel](#)

[Previous](#)

[Next: Review](#)

Click **Create User**.

7. Click **Download .csv** for downloading a CSV file containing the security credentials and then click **Close**:

The screenshot shows the 'Create User' dialog box with the following details:

- Success:** You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.
- Download .csv:** A button to download the CSV file.
- User Table:** A table showing the newly-created user 'John'.

	User	Access key ID	Secret access key	Password	Email login instructions
▶	✓ John	AKIARQNEQ73XQHF2RTH	***** Show	***** Show	<input type="checkbox"/> Send email
- Close:** A button to close the dialog.

Review the newly-created user in the **IAM Console**:

The screenshot shows the AWS IAM 'Users' list. A green success message at the top states: 'The user John have been created.' Below this, the 'Users (3)' section is displayed. The table has columns for User name, Groups, Last activity, MFA, and Password last used. The 'User name' column includes checkboxes. The data is as follows:

User name	Groups	Last activity	MFA	Password last used
John	None	Never	None	Now
main_service_account_user	None	Never	None	None
student	None	17 minutes ago	None	None

At the bottom of the page, the footer includes links for Privacy, Terms, and Cookie preferences, along with system status icons and the date/time (25-Nov-2021, 21:08 IN).

Click **User groups > DevOps** to open the DevOps group details view:

The screenshot shows the 'User groups > DevOps' details view. The left sidebar shows 'Identity and Access Management (IAM)' with 'User groups' selected. The main content area shows the 'DevOps' group summary. The 'Summary' table includes fields for User group name (DevOps), Creation time (November 25, 2021, 21:01 (UTC+05:30)), and ARN (arn:aws:iam::103961132789:group/DevOps). Below the summary is a tab navigation bar with 'Users' (selected), 'Permissions', and 'Access Advisor'. The 'Users in this group (0)' section indicates that no users are currently assigned to this group. At the bottom, the footer includes links for Privacy, Terms, and Cookie preferences, along with system status icons and the date/time (25-Nov-2021, 21:09 IN).

Click **Add Users**.

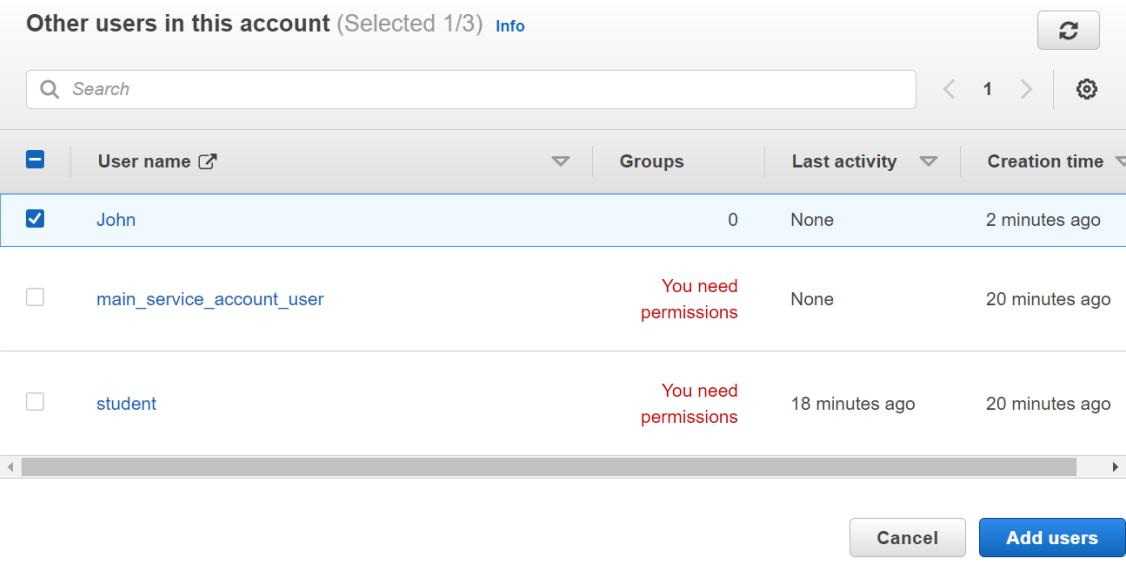
11. Check **John** and click **Add Users**:

Add users to DevOps

Other users in this account (Selected 1/3) [Info](#)

User name	Groups	Last activity	Creation time
<input checked="" type="checkbox"/> John	0	None	2 minutes ago
<input type="checkbox"/> main_service_account_user	You need permissions	None	20 minutes ago
<input type="checkbox"/> student	You need permissions	18 minutes ago	20 minutes ago

[Cancel](#) [Add users](#)



Observe that John is now in the DevOps group:

The screenshot shows the AWS IAM User page. At the top, there's a summary section with details: User group name (DevOps), Creation time (November 25, 2021, 21:01 (UTC+05:30)), and ARN (arn:aws:iam::103961132789:group/DevOps). Below this, there are tabs for 'Users' (selected), 'Permissions', and 'Access Advisor'. The 'Users in this group' section shows one user, 'John', with a search bar and pagination controls. The bottom of the page includes standard AWS navigation links and a footer with copyright information and system status.

Logging in using the new IAM credentials

click on **Users** in the sidebar menu.Click **John** on the **IAM User** page:

Click **Security Credentials** and then navigate to the **Console sign-in link** listed in the tab:

The screenshot shows the AWS IAM User page for user 'John'. The left sidebar has 'Identity and Access Management (IAM)' selected, with 'Users' also highlighted. The main area shows the 'Summary' tab for user 'John'. The 'Security credentials' tab is selected, showing the 'Sign-in credentials' section. It lists the 'Console sign-in link' as <https://103961132789.sigin.aws.amazon.com/console>. Other sections include 'Console password' (Enabled), 'Assigned MFA device' (Not assigned), and 'Signing certificates' (None). The bottom of the page includes standard AWS navigation links and a footer with copyright information and system status.

Use the credentials in the CSV file you downloaded to log in as John.



Sign in as IAM user

Account ID (12 digits) or account alias

103961132789

IAM user name

John|

Password

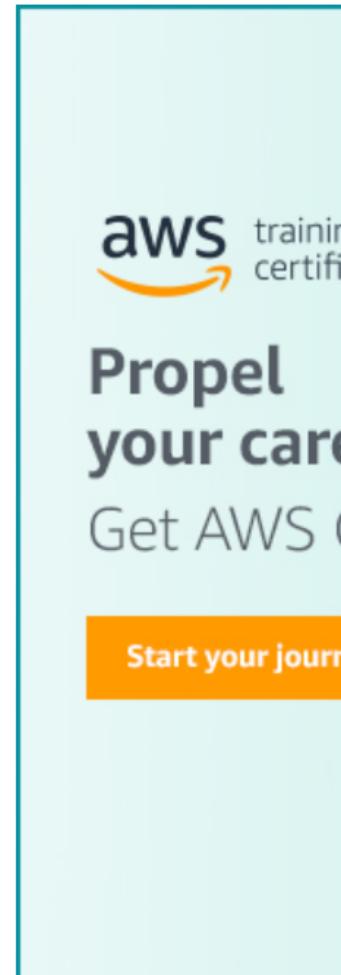
.....

Remember this account

Sign in

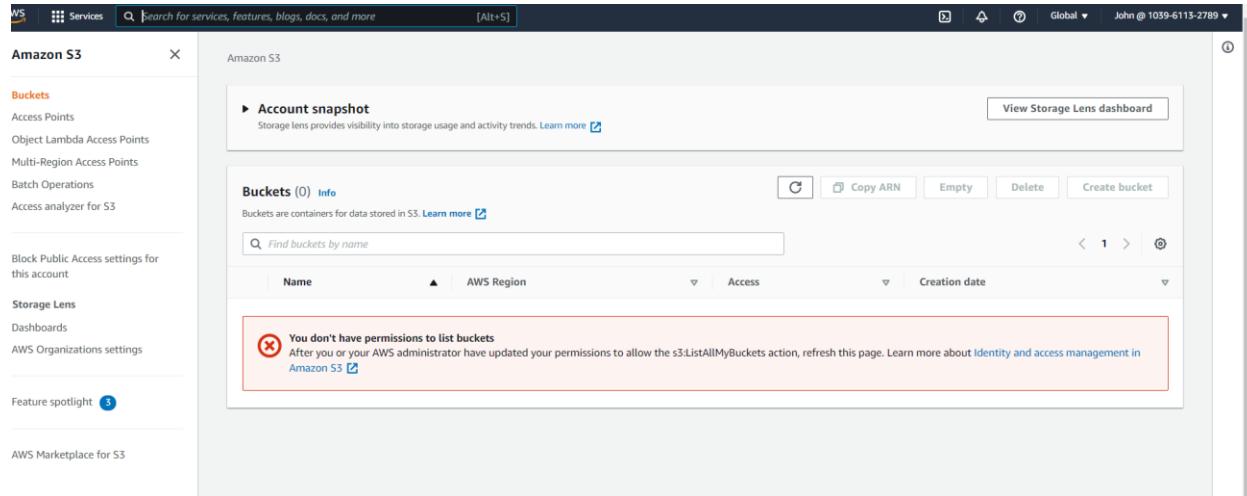
[Sign in using root user email](#)

[Forgot password?](#)



From the AWS Management Console, click on **Services** at the top of the page and type **S3** into the text box. Select the **S3** option:

- . Notice that due to the restrictive permissions you placed on the IAM user "John", you receive an **Access Denied** message when attempting to access S3 resources:



Practical No. 3

Working With S3 Buckets

Aim: A) Create a bucket

- B) Upload an object to the bucket
- C) Make an object public
- D) Create a bucket policy
- E) Explore versioning

Introduction to CloudWatch

Lab Steps

Logging in to the Amazon Web Services Console

Explore CloudWatch

Monitoring EC2 Instances

Install the EC2 Monitoring Scripts

Creating Your First CloudWatch Alarm

Create an Alarm using the EC2 console

Sharing CloudWatch Metrics with others

A) Create a bucket

Step 1: Click on Start Lab

← Introduction to Amazon Simple Storage Service (S3)

Start Lab

01:30:00

Introduction to Amazon Simple Storage Service (S3)

1 hour 30 minutes

Free

★★★★★ Rate Lab



← Introduction to Amazon Simple Storage Service (S3)

End Lab

01:26:13

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](#)

[Download PEM](#)

[Download PPK](#)

Task 1: Create a bucket

You are new to Amazon S3 and want to test the features and security of S3 as you configure the environment to hold the EC2 report data. You know that every object in Amazon S3 is stored in a bucket so creating a new bucket to hold the reports is the first thing on your task list.

In this task, you create a bucket to hold your EC2 report data and then examine the different bucket configuration options.

- At the top-left of the AWS Management Console, on the **Services** menu choose S3.

You can also search for S3 at the top of the services menu.

[Start Lab](#)

Task 1: Create a bucket

Task 2: Upload an object to the bucket

Task 3: Make an object public

Task 4: Test connectivity from the EC2 instance

Task 5: Create a bucket policy

Task 6: Explore versioning

Summary:

Step 2 : Open YOu lab by choosing Open Console

AWS Management Console

AWS services

▼ Recently visited services
Your recently visited AWS services appear here.

► All services

Stay connected to your AWS resources on-the-go

 AWS Console Mobile App now supports four additional regions. Download the AWS Console Mobile App to your iOS or Android mobile device. [Learn more](#)

Explore AWS

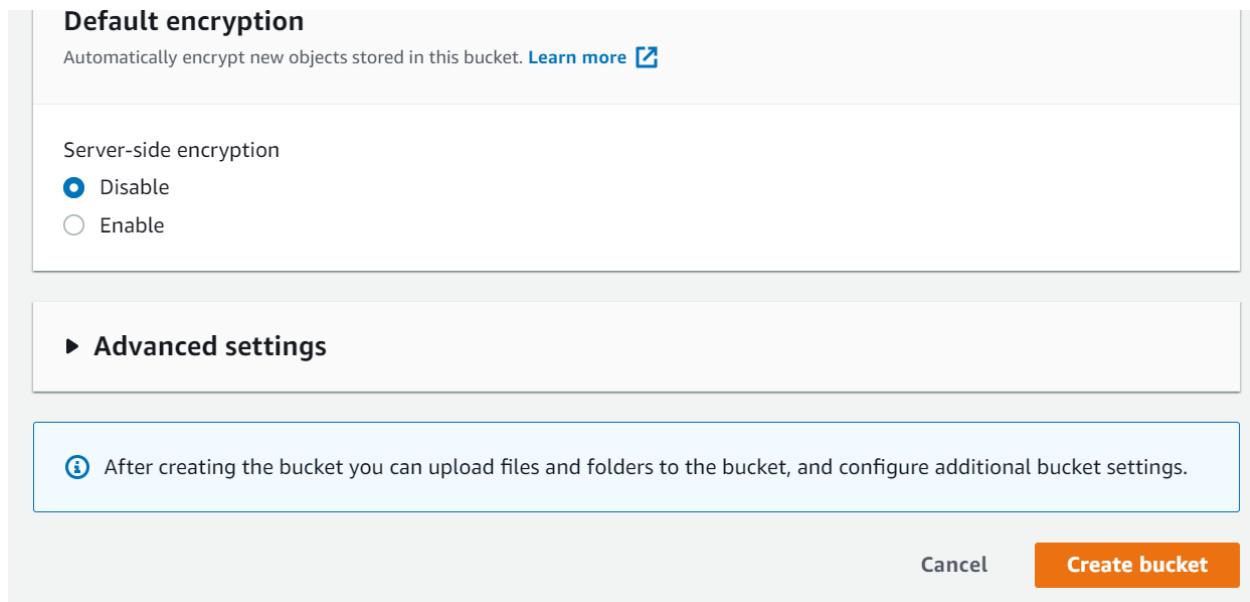
Step 3 : At the top of the menu- click on services menu and choose s3

<p>Serverless Application Repository</p> <p>AWS Outposts</p> <p>EC2 Image Builder</p> <p>AWS App Runner</p> <p> Containers</p> <ul style="list-style-type: none">Elastic Container RegistryElastic Container ServiceElastic Kubernetes ServiceRed Hat OpenShift Service on AWS <p> Storage</p> <ul style="list-style-type: none">S3EFSFSxS3 GlacierStorage GatewayAWS Backup <p> Database</p>	<p>Amazon Forecast</p> <p>Amazon Fraud Detector</p> <p>Amazon Kendra</p> <p>Amazon Lex</p> <p>Amazon Personalize</p> <p>Amazon Polly</p> <p>Amazon Rekognition</p> <p>Amazon Textract</p> <p>Amazon Transcribe</p> <p>Amazon Translate</p> <p>AWS DeepComposer</p> <p>AWS DeepLens</p> <p>AWS DeepRacer</p> <p>AWS Panorama</p> <p>Amazon Monitron</p> <p>Amazon HealthLake</p> <p>Amazon Lookout for Vision</p> <p>Amazon Lookout for Equipment</p> <p>Amazon Lookout for Metrics</p>	<p>tomorrow. Find out now. Learn more</p> <p>Free AWS Training Advance your career with AWS Cloud Practitioner Essentials—a free, six-hour, foundational course. Learn more</p> <p>AWS Certification Propel your career forward with AWS Certification. Learn more</p> <p>AWS Training Free digital courses to help you develop your skills. Learn more</p> <p>Have feedback?</p>
---	--	---

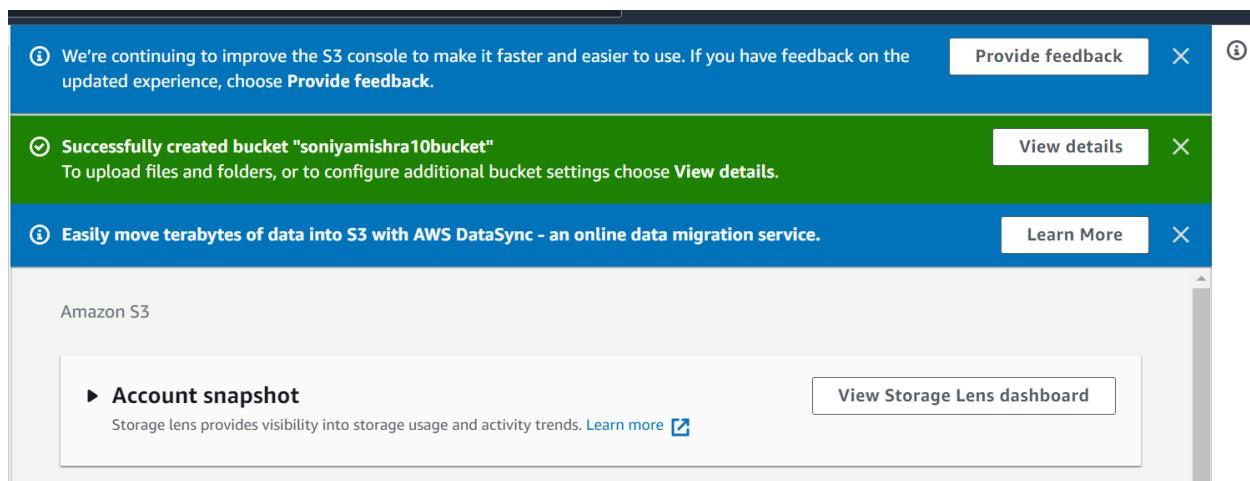
The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with navigation links like 'Buckets', 'Access Points', 'Object Lambda Access Points', etc. The main area displays a message about improving the console, followed by another message about AWS DataSync. Below these messages is a table titled 'Buckets (2)'. The table has columns for Name, AWS Region, Access, and Creation date. It lists two buckets: 'ql-cf-templates-1634183066-581f97a08c75e166-us-west-2' (US West (Oregon), us-west-2, public, Oct 14, 2021) and 'qltrail-lab-2543-1634183069' (US East (N. Virginia), us-east-1, public, Oct 14, 2021). A prominent orange 'Create bucket' button is located at the top right of the table area.

Step 4 : Click on Create bucket button

The screenshot shows the 'Create bucket' configuration page. At the top, there's a blue header bar with a message about improving the S3 console. Below the header, the page title is 'Create bucket' with an 'Info' link. A sub-header states 'Buckets are containers for data stored in S3.' with a 'Learn more' link. The main form is titled 'General configuration'. It contains fields for 'Bucket name' (with the value 'soniyamishra10bucket' highlighted in a blue box) and 'AWS Region' (set to 'US West (Oregon) us-west-2'). There's also a note about copying settings from an existing bucket.



Step 5: Give a unique Bucket Name and scroll down and click on create bucket button



Bucket is successfully created

B) Upload an object to the bucket

Step 1: Choose your bucket and click the upload button

We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose [Provide feedback](#).

Objects (0)

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

Action Buttons: C Copy S3 URI, Copy URL, Download, Open, Delete, Actions ▾, Create folder, Upload.

Search Bar: Find objects by prefix.

Table Headers: Name, Type, Last modified, Size, Storage class.

No objects

You don't have any objects in this bucket.

Upload Button: Click to upload files.

Files and folders (1 Total, 84.0 KB)

All files and folders in this table will be uploaded.

Action Buttons: Remove, Add files, Add folder.

Search Bar: Find by name.

Table Headers: Name, Folder, Type, Size.

Name	Folder	Type	Size
new-report.png	-	image/png	84.0 KB

Destination

Destination
<s3://soniyamishra10bucket>

Destination details

Bucket settings that impact new objects stored in the specified destination

Step 2: click on Add files and browse and choose your file and upload

The screenshot shows the AWS S3 console. At the top, a green banner displays a success message: "Upload succeeded" with a checkmark icon, followed by "View details below." Below the banner, there is a summary table with three columns: "Destination" (s3://soniyamishra10buckets), "Succeeded" (1 file, 84.0 KB (100.00%)), and "Failed" (0 files, 0 B (0%)). Below the table, there are two tabs: "Files and folders" (which is selected) and "Configuration". Under the "Files and folders" tab, a table lists one file: "new-report.png" (image/png, 84.0 KB, Status: Succeeded). A search bar and navigation icons are also visible.

Your file has been successfully uploaded

C) Make an object public

Step 1: click on the file you have uploaded to the bucket and you will be redirected to the Object Overview page , locate the link of Object url copy and paste to a new tab

You will receive an Access Denied Error, because S3 bucket object are bydefault private.

S https://soniyamishra10buckets.s3.us-west-2.amazonaws.com/new-report.png

Managed bookmarks India Intranet Home AWS Management... What is a core char... Applied eC: MuleSo... Anypoint Platform

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

```
▼<Error>
<Code>AccessDenied</Code>
<Message>Access Denied</Message>
<RequestId>GDP4PNX8DRCY0FH</RequestId>
<HostId>CbgrzovGYZjg/I2ERjvWxRPx1ATKYPN1f0hdgeGWZAaI2fW/49NXm28qlvwKnY2QGzUUquBUD+E=</HostId>
</Error>
```

amazon S3 > soniyamishra10buckets > new-report.png

new-report.png Info

Properties Permissions Versions

Object overview

Owner aws088650	S3 URI s3://soniyamishra10buckets/new-report.png
AWS Region US West (Oregon) us-west-2	Amazon Resource Name (ARN) arn:aws:s3:::soniyamishra10buckets/new-report.p
Last modified October 14, 2021, 11:25:01 (UTC+05:30)	Entity tag (Etag) 75acf5a0dd2f6bdd67c36fa2748a1a19
Size 84.0 KB	Object ID Object ID

Object actions ▾

- Download as
- Calculate total size
- Copy
- Move
- Initiate restore
- Query with S3 Select
- Edit actions
- Rename object
- Edit storage class
- Edit server-side encryption
- Edit metadata
- Edit tags
- Make public**

Step 2: In the object overview(new-report.png) page of the click on object action and click on make public

Make public Info

The make public action enables public read access in the object access control list (ACL) settings. [Learn more](#)



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](#)



When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

Specified objects

Find objects by name

< 1 >

Name	Type	Last modified	Size
new-report.png	png	October 14, 2021, 11:25:01 (UTC+05:30)	84.0 KB

Cancel

Make public

Click on make public

Failed to edit public access
For more information, see the Error column in the Failed to edit table below.

Make public: status



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](#)

The information below will no longer be available after you navigate away from this page.

Summary

Source
s3://soniyamishra10buckets

Successfully edited public access
0 objects

Failed to edit public access
 1 object, 84.0 KB

[Failed to edit public access](#)

[Configuration](#)

Failed to edit public access (1 object, 84.0 KB)

You will be failed to make public

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with the AWS logo, a 'Services' dropdown, a search bar containing 'Search for services, features, marketplace products, and docs [Alt+S]', and a user icon. Below the navigation bar, the path 'Amazon S3 > soniyamishra10buckets' is shown. The main title is 'soniyamishra10buckets' with an 'Info' link. A horizontal menu bar below the title includes 'Objects', 'Properties', 'Permissions' (which is highlighted in orange), 'Metrics', 'Management', and 'Access Points'. The 'Permissions' section is expanded, showing a 'Permissions overview' header and a 'Access' section indicating 'Bucket and objects not public'. Below this, the 'Block public access (bucket settings)' section is expanded, showing a note about public access settings, an 'Edit' button, and a 'Block all public access' setting which is currently 'On'. A sub-section under 'Block all public access' is titled 'Block public access to buckets and objects granted through new access control lists (ACLs)'. The entire screenshot is framed by a thick black border.

Step 3: Come back to bucket page and go to permissions and go to edit of Block public access section

EDIT BLOCK PUBLIC ACCESS (BUCKET SETTINGS) Info

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](#)

Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

Block public access to buckets and objects granted through new public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

Block public and cross-account access to buckets and objects through any public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

[Cancel](#)

[Save changes](#)

Step 4: Uncheck block all public access

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](#)

Block all public access

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

Block public access to buckets and objects granted through new access control lists (ACLs)

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

Block public access to buckets and objects granted through any access control lists (ACLs)

S3 will ignore all ACLs that grant public access to buckets and objects.

Block public access to buckets and objects granted through new public bucket or access point policies

S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.

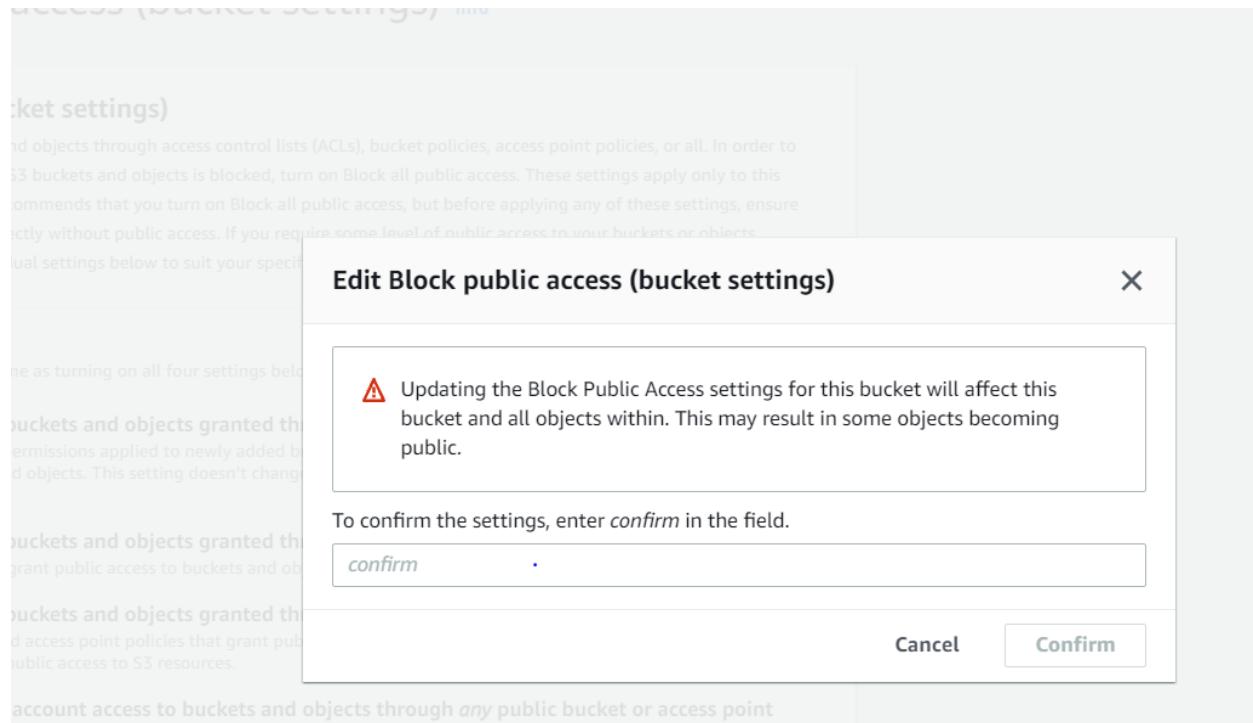
Block public and cross-account access to buckets and objects through any public bucket or access point policies

S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

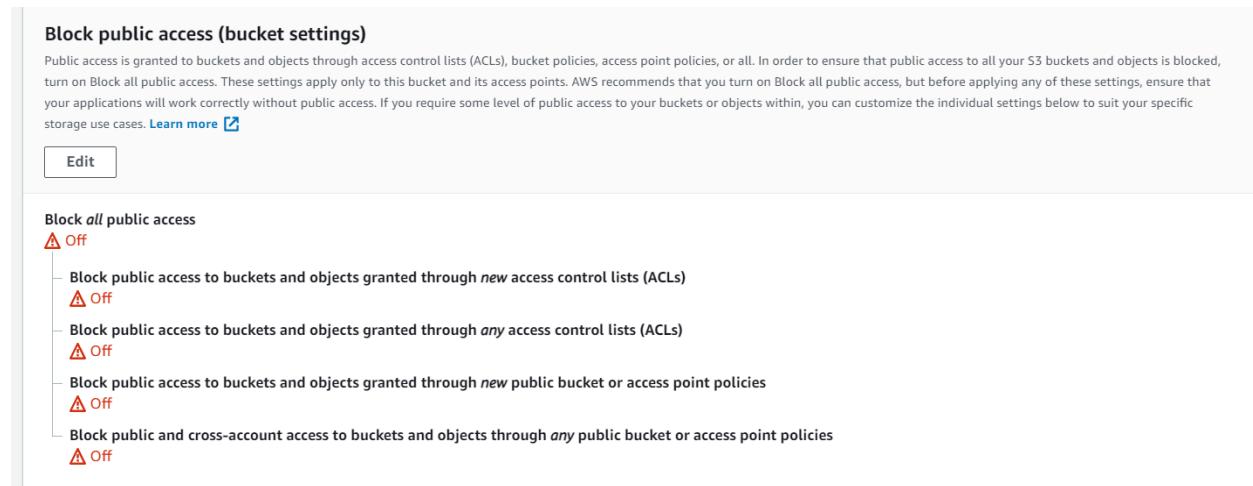
[Cancel](#)

[Save changes](#)

and click on save changes button



Write “confirm” on the textbox



Amazon S3 > soniyamishra10bucket > new-report.png

new-report.png [Info](#)

[Properties](#) [Permissions](#) [Versions](#)

Object overview

Owner	S3 URI
aws088629	s3://soniyamishra10bucket/new-report.png
AWS Region	Amazon Resource Name (ARN)
US West (Oregon) us-west-2	arn:aws:s3:::soniyamishra10bucket/new-report.png
Last modified	Entity tag (Etag)
October 14, 2021, 14:25:04 (UTC+05:30)	75acf5a0dd2f6bdd67c36fa2748a1a19
Size	Object URL
84.0 KB	https://soniyamishra10bucket.s3.us-west-2.amazonaws.com/new-report.png
Type	
png	
KPIs	

Object actions ▲

- Download as
- Calculate total size
- Copy
- Move
- Initiate restore
- Query with S3 Select
- Edit actions**
- Rename object
- Edit storage class
- Edit server-side encryption
- Edit metadata
- Edit tags
- Make public

[Amazon S3](#) / [soniyamishra10bucket](#) / [new-report.png](#)

Make public [Info](#)

The make public action enables public read access in the object access control list (ACL) settings. [Learn more](#).

⚠ When public read access is enabled and not blocked by Block Public Access settings, anyone in the world can access the specified objects.

Specified objects

Name	Type	Last modified	Size
new-report.png	png	October 14, 2021, 14:25:04 (UTC+05:30)	84.0 KB

[Cancel](#) [Make public](#)

Successfully edited public access
View details below.

Make public: status

The information below will no longer be available after you navigate away from this page.

Summary	
Source s3://soniyamishra10bucket	Successfully edited public access 1 object, 84.0 KB
	Failed to edit public access 0 objects

new-report.png [Info](#)

[Properties](#) [Permissions](#) [Versions](#)

Object overview

Owner	s3://soniyamishra10bucket/new-report.png
AWS Region	Amazon Resource Name (ARN)
US West (Oregon) us-west-2	arn:aws:s3:::soniyamishra10bucket/new-report.png
Last modified	Entity tag (Etag)
October 14, 2021, 14:25:04 (UTC+05:30)	75acf5a0dd2f6bdd67c36fa2748a1a19
Size	Object URL Copied
84.0 KB	https://soniyamishra10bucket.s3.us-west-2.amazonaws.com/new-report.png
Type	
png	
Key	
new-report.png	

[new-report.png \(1045x602\)](#)

soniyamishra10bucket.s3.us-west-2.amazonaws.com/new-report.png

Managed bookmarks India Intranet Home... AWS Management... What is a core char... Applied eC: MuleSoft Anypoint Platform Other books

File Home Insert Page Layout Formulas Data Review View Help Tell me what you want to do

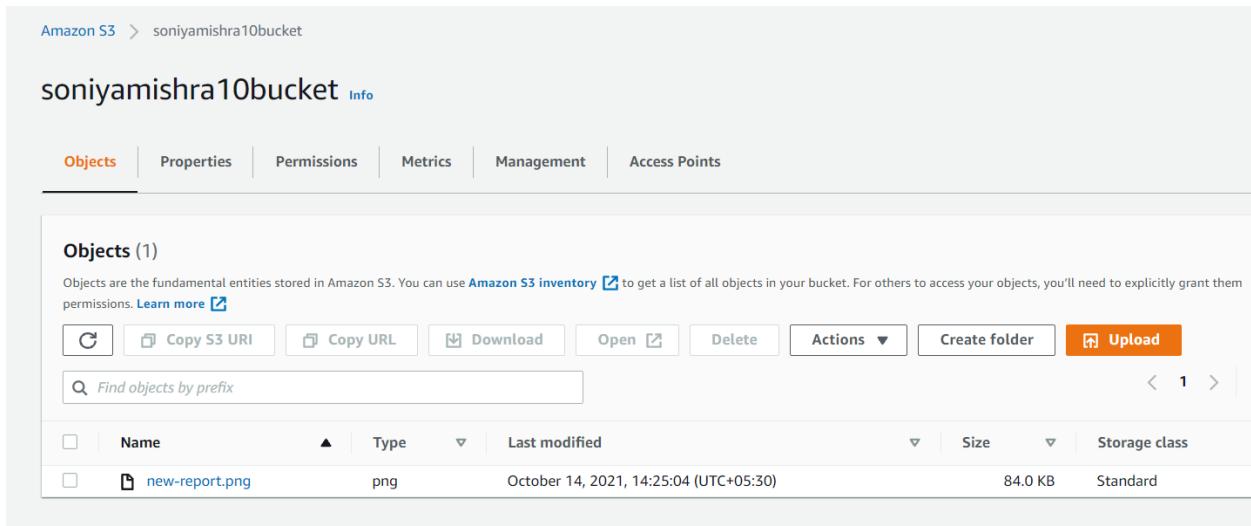
A18

Service	Operation	UsageType	Resource	StartTime	EndTime	UsageValue
AmazonS3	HeadBucket	USW2-C3DataTransfer-Out-Bytes	lab-test-bucket-77	10/31/2020 0:00	12/31/2020 11:59	15309
AmazonS3	PutObject	USW2-C3DataTransfer-In-Bytes	admin-test-77	10/31/2020 0:00	12/31/2020 11:59	19032
AmazonS3	HeadBucket	USW2-Requests-Tier2	admin-test-77	10/31/2020 0:00	12/31/2020 11:59	128
AmazonS3	PutObjectForReplication	USW1-Requester-SIA-Tier1	mybucket-98765	10/31/2020 0:00	12/31/2020 11:59	56888
AmazonS3	GetObjectFor Replication	USW1-USW2-AWS-In-Bytes	mybucket-98766	10/31/2020 0:00	12/31/2020 11:59	254587
AmazonS3	GetObjectFor Replication	USW2-C3DataTransfer-Out-Bytes	mybucket-98767	10/31/2020 0:00	12/31/2020 11:59	235
AmazonS3	HeadBucket	USW2-C3DataTransfer-In-Bytes	mybucket-98768	10/31/2020 0:00	12/31/2020 11:59	25589

Now you can refresh the page and able to view the file

Task 5: Create a bucket Policy

Step 1 At the top of the menu- click on services menu and choose s3



The screenshot shows the Amazon S3 console interface. The top navigation bar includes 'Amazon S3' and the bucket name 'soniyamishra10bucket'. Below the navigation, there are tabs for 'Objects' (which is selected), 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. The main content area is titled 'Objects (1)'. It displays a single object named 'new-report.png' with the following details:

Name	Type	Last modified	Size	Storage class
new-report.png	png	October 14, 2021, 14:25:04 (UTC+05:30)	84.0 KB	Standard

Below the table are several actions: 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', 'Actions', 'Create folder', and 'Upload' (highlighted in orange). There is also a search bar labeled 'Find objects by prefix'.

Step 2 Choose you bucket and click the upload button

Upload Info

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 folder**.

Files and folders (1 Total, 113.0 B)

All files and folders in this table will be uploaded.

[Remove](#)

[Add files](#)

[Add folder](#)

Find by name

< 1 >

<input type="checkbox"/>	Name	Folder	Type	Size
<input type="checkbox"/>	sample-file.txt	-	text/plain	113.0 B

Destination

Step 3: click on Add files and browse and choose your file and upload

Upload succeeded
View details below.

Upload: status [Close](#)

The information below will no longer be available after you navigate away from this page.

Summary		
Destination	Succeeded	Failed
s3://soniyamishra10bucket	1 file, 113.0 B (100.00%)	0 files, 0 B (0%)

[Files and folders](#) [Configuration](#)

Uploaded successfully

The screenshot shows the 'Object overview' page for a file named 'sample-file.txt' in the 'soniyamishra10bucket' bucket. The top navigation bar includes 'Amazon S3 > soniyamishra10bucket > sample-file.txt'. Below the navigation are buttons for 'Copy S3 URI', 'Download', 'Open', and 'Object actions'. A tab bar at the top of the main content area shows 'Properties' (selected), 'Permissions', and 'Versions'. The 'Object overview' section contains the following details:

Property	Value
Owner	aws088629
AWS Region	US West (Oregon) us-west-2
Last modified	October 14, 2021, 14:40:23 (UTC+05:30)
Size	113.0 B
Type	txt
S3 URI	s3://soniyamishra10bucket/sample-file.txt
Amazon Resource Name (ARN)	arn:aws:s3:::soniyamishra10bucket/sample-file.txt
Entity tag (Etag)	4a0b2a536384728d06b8a9c5ceae0581
Object URL	https://soniyamishra10bucket.s3.us-west-2.amazonaws.com/sample-file.txt

Step 4

click on the file you have uploaded to the bucket and you will be redirected to the Object Overview page , locate the link of Object url copy and paste to a new tab

You will receive an Access Denied Error, because S3 bucket object are by default private.

← → ⌂ ⌂ soniyamishra10bucket.s3.us-west-2.amazonaws.com/sample-file.txt

_apps Managed bookmarks India Intranet Hom... AWS Management... What is a core char... Applied eC...

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

```
▼<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>MW7PVQ8AHM20AH11</RequestId>
  <HostId>9W6TF1SFjMC6kiMQUB86s9t12Dg2RJ2wahORo80BN/XcR7Z71S/0dwBdueSGL6r5nKTzPC/ogag=</HostId>
</Error>
```

The screenshot shows the AWS Management Console with the search bar set to 'roles'. The left sidebar is the 'Amazon S3' service, with 'Buckets' expanded to show 'Access Points', 'Object Lambda Access', 'Multi-Region Access P...', 'Batch Operations', and 'Access analyzer for S3'. Below that is 'Block Public Access settings for this account'. Under 'Storage Lens', there are 'Dashboards' and 'AWS Organizations settings'. A 'Feature spotlight' section is also present. The main content area is titled 'Services' and lists 'IAM' (selected), 'Documentation (70,937)', 'Knowledge Articles (30)', and 'Marketplace (495)'. Under 'Features', there are sections for 'Roles' (with 'IAM feature'), 'SiteWise Monitor' (with 'IoT SiteWise feature'), and 'Policies' (with 'IAM feature'). On the right, there is a preview pane showing a file named 'sample-file.txt' with details like size (84.0 KB, 113.0 B) and storage class (Standard). The bottom navigation bar includes links for 'Feedback', 'English (US)', 'Privacy Policy', 'Terms of Use', and 'Cookie preferences'. The system tray at the bottom shows the date (14-10-2021), time (14:45), battery level (Haze), and network status (34°C).

Step 5 : Go to

Services

>IAM > Roles.

The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, there's a navigation sidebar with options like Dashboard, Access management, Policies, and Roles. The 'Roles' option is currently selected. The main content area is titled 'Roles (18) Info' and contains a search bar with the query 'EC2InstanceProfileRole'. Below the search bar, a table lists one role: 'EC2InstanceProfileRole' under the 'Trusted entities' column, which is described as 'AWS Service: ec2'. There are buttons for 'Create role', 'Delete', and a refresh icon.

Step 5 Select EC2InstanceProfileRole. On the Summary page, copy the Role ARN to a text file to be used in a later step.

Select EC2InstanceProfileRole. On the Summary page, copy the Role ARN to a text file to be used in a later step.

It should look similar to this: arn:aws:iam::596123517671:role/EC2Instan

Step 6: Choose Services S3 and return to the s3 Management Console.

The screenshot shows the AWS S3 console. At the top, there is a search bar with the placeholder "Search for services, features, marketplace products, and docs" and a keyboard shortcut "[Alt+S]". To the right of the search bar are user information and navigation links for "Global". Below the header, the page title "Amazon S3" is displayed. A section titled "Account snapshot" provides summary statistics: Total storage (4.8 MB), Object count (33), and Avg. object size (148.4 KB). It also includes a note about enabling advanced metrics. A "View Storage Lens dashboard" button is located in the top right corner of this section. The main content area is titled "Buckets (3) Info". It contains a sub-header stating "Buckets are containers for data stored in S3." Below this is a search bar with the placeholder "Find buckets by name". A table lists three buckets: "ql-cf-templates-1634201394-7213c174eb04f30c-us-west-2" (US West (Oregon) us-west-2, Objects can be public, created Oct 14, 2021), "qltrail-lab-2543-1634201397" (US East (N. Virginia) us-east-1, Objects can be public, created Oct 14, 2021), and "soniyamishra10bucket" (US West (Oregon) us-west-2, Objects can be public, created Oct 14, 2021). Action buttons for "Copy ARN", "Empty", "Delete", and "Create bucket" are located at the top right of the table.

Step 7 : Choose your bucket.

You should see the two objects you uploaded

Click on permission tab scroll down and click on edit section of Bucket policy editor

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

⚠ Off

- Block public access to buckets and objects granted through *new* access control lists (ACLs)
⚠ Off
- Block public access to buckets and objects granted through *any* access control lists (ACLs)
⚠ Off
- Block public access to buckets and objects granted through *new* public bucket or access point policies
⚠ Off
- Block public and cross-account access to buckets and objects through *any* public bucket or access point policies
⚠ Off

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

[Edit](#) [Delete](#)

No policy to display.

[Copy](#)

Amazon S3 > soniyamishra10bucket > Edit bucket policy

Edit bucket policy [Info](#)

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#)

[Policy examples](#) [Policy generator](#)

Bucket ARN

[Bucket ARN copied](#)

Policy

```
1 |
```

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an [IAM Policy](#), an [S3 Bucket Policy](#), an [SNS Topic Policy](#), a [VPC Endpoint Policy](#), and an [SQS Queue Policy](#).

Select Type of Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

Effect Allow Deny

Principal

Use a comma to separate multiple values.

AWS Service All Services ('*')

Use multiple statements to add permissions for more than one service.

Actions All Actions ('*')

Amazon Resource Name (ARN)

ARN should follow the following format: arn:aws:s3:::\${BucketName}/\${KeyName}.

Use a comma to separate multiple values.

Add Conditions (Optional)

Add Conditions (Optional)

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource	Conditions
• arn:aws:iam::109836276268:role/EC2InstanceProfileRole	Allow	• s3:GetObject • s3:PutObject	arn:aws:s3:::soniyamishra10bucket/*	None

Step 3: Generate Policy

A *policy* is a document (written in the [Access Policy Language](#)) that acts as a container for one or more statements.

[Start Over](#)

Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor.
Changes made below will not be reflected in the policy generator tool.

```
{  
    "Id": "Policy1634203732430",  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Sid": "Stmt1634203670252",  
            "Action": [  
                "s3:GetObject",  
                "s3:PutObject"  
            ],  
            "Effect": "Allow",  
            "Resource": "arn:aws:s3:::soniyamishra10bucket/*",  
            "Principal": {  
                "AWS": [  
                    "arn:aws:iam::109836276268:role/EC2InstanceProfileRole"  
                ]  
            }  
        }  
    ]  
}
```

Close

The screenshot shows the 'Edit bucket policy' page for the 'soniyamishra10bucket' bucket in the Amazon S3 console. The left sidebar has a tree view with nodes like 'Access Points', 'AWS Points', 'S3', 'Settings for S3', and a circled '3'. The main content area has a breadcrumb trail: 'Amazon S3 > soniyamishra10bucket > Edit bucket policy'. The title is 'Edit bucket policy' with an 'Info' link. Below it is a 'Bucket policy' section with a note about bucket policies being JSON files that provide access to objects in the bucket. It includes 'Policy examples' and 'Policy generator' buttons. The 'Policy' section displays the following JSON code:

```
1  {
2   "Id": "Policy1634203732430",
3   "Version": "2012-10-17",
4   "Statement": [
5     {
6       "Sid": "Stmt1634203670252",
7       "Action": [
8         "s3:GetObject",
9         "s3:PutObject"
10      ],
11      "Effect": "Allow",
12      "Resource": "arn:aws:s3:::soniyamishra10bucket/*",
13      "Principal": {
14        "AWS": [
15          "arn:aws:iam:109836276268:role/EC2InstanceProfileRole"
16        ]
17      }
18    }
19  ]
20 }
```

The screenshot shows the AWS S3 console with the bucket 'soniyamishra10bucket'. The 'Permissions' tab is selected. It displays that objects can be public. A section titled 'Block public access (bucket settings)' indicates that all public access is off. There is an 'Edit' button available for modifying these settings.

The screenshot shows the AWS search results for 'ec2'. The search bar at the top contains 'ec2'. The results are categorized under 'Services (7)'. The first result is 'EC2: Virtual Servers in the Cloud'. Below it are 'EC2 Image Builder', 'EC2 Global View', and 'AWS Compute Optimizer'. At the bottom, there is a 'Features' section with a link to 'See all 35 results'.

The screenshot shows the AWS Management Console with the search bar set to 'ec2'. The main content area displays the 'Resources' section, which lists the following Amazon EC2 resources in the US West (Oregon) Region:

Instances (running)	1
Dedicated Hosts	0
Elastic IPs	0
Instances	1
Key pairs	1
Load balancers	0
Placement groups	0
Security groups	3
Snapshots	0
Volumes	1

A tooltip message at the bottom left of the resources section states: "Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. [Learn more](#)".

The sidebar on the left includes links for 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Tags', 'Limits', and sections for 'Instances' (with sub-links for 'Instances', 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', and 'Scheduled Instances').

The right sidebar contains sections for 'Account attributes' (with a 'Edit' button), 'Supported platforms' (listing 'VPC'), 'Default VPC' (set to 'vpc-be64dcc6'), 'Settings', 'EBS encryption', 'Zones', 'EC2 Serial Console', 'Default credit specification', and 'Console experiments'.

The screenshot shows the 'Instances' page with 1 running instance. The table displays the following information for the single instance:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availab...
Bastion Host	i-06a75dab13a74f24f	Running	t3.micro	2/2 checks passed	OK	us-v...

Filtering options include 'Instance state: running' and 'Clear filters'. Action buttons include 'Launch instances' and 'Actions'.



Services ▾

Q ec2



awss



EC2 > Instances > i-06a75dab13a74f24f > Connect to instance

Connect to instance Info

Connect to your instance i-06a75dab13a74f24f (Bastion Host) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 Serial Console

Session Manager usage:

- Connect to your instance without SSH keys or a bastion host.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) page.

Cancel

Connect

```
sh-4.2$ cd ~
sh-4.2$ pwd
/home/ssm-user
sh-4.2$ aws s3 ls
2021-10-14 08:49:56 ql-cf-templates-1634201394-7213c174eb04f30c-us-west-2
2021-10-14 08:49:58 qltrail-lab-2543-1634201397
2021-10-14 08:54:22 soniyamishra10bucket
sh-4.2$ aws s3 ls s3://soniyamishra10bucket
2021-10-14 08:55:04      86065 new-report.png
2021-10-14 09:10:23      113 sample-file.txt
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$ pwd
/home/ssm-user/reports
sh-4.2$ aws s3 ls s3://soniyamishra10bucket
2021-10-14 08:55:04      86065 new-report.png
2021-10-14 09:10:23      113 sample-file.txt
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://soniyamishra10bucket
upload: ./report-test1.txt to s3://soniyamishra10bucket/report-test1.txt
sh-4.2$ aws s3 ls s3://soniyamishra10bucket
2021-10-14 08:55:04      86065 new-report.png
2021-10-14 10:05:14      31 report-test1.txt
2021-10-14 09:10:23      113 sample-file.txt
sh-4.2$ aws s3 cp s3://reportbucket(NUMBER)/sample-file.txt sample-file.txt
sh: syntax error near unexpected token `('
sh-4.2$ aws s3 cp s3://soniyamishra10bucket/sample-file.txt sample-file.txt
```

```
dolphins.jpg  files.zip  report-test1.txt  report-test2.txt  report-test3.txt  whale.jpg
sh-4.2$ pwd
/home/ssm-user/reports
sh-4.2$ aws s3 ls s3://soniyamishra10bucket
2021-10-14 08:55:04      86065 new-report.png
2021-10-14 09:10:23      113 sample-file.txt
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://soniyamishra10bucket
upload: ./report-test1.txt to s3://soniyamishra10bucket/report-test1.txt
sh-4.2$ aws s3 ls s3://soniyamishra10bucket
2021-10-14 08:55:04      86065 new-report.png
2021-10-14 10:05:14      31 report-test1.txt
2021-10-14 09:10:23      113 sample-file.txt
sh-4.2$ aws s3 cp s3://reportbucket(NUMBER)/sample-file.txt sample-file.txt
sh: syntax error near unexpected token `('
sh-4.2$ aws s3 cp s3://soniyamishra10bucket/sample-file.txt sample-file.txt
download: s3://soniyamishra10bucket/sample-file.txt to ./sample-file.txt
sh-4.2$ ls
dolphins.jpg  files.zip  report-test1.txt  report-test2.txt  report-test3.txt  sample-file.txt  whale.jpg
sh-4.2$ █
```

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

```
▼<Error>
  <Code>AccessDenied</Code>
  <Message>Access Denied</Message>
  <RequestId>MW7PVQ8AHM20AH11</RequestId>
  <HostId>9W6TF1SFjMC6kiMQUB86s9t12Dg2RJ2wah0Ro80BN/XcR7Z71S/0dwBdueSGL6r5nKTzPC/ogag=</HostId>
</Error>
```

Policy

```
1 [ {
  2   "Version": "2012-10-17",
  3   "Id": "Policy1634203732430",
  4   "Statement": [
  5     {
  6       "Sid": "Stmt1634203670252",
  7       "Effect": "Allow",
  8       "Principal": {
  9         "AWS": "arn:aws:iam::109836276268:role/EC2InstanceProfileRole"
 10      },
 11       "Action": [
 12         "s3:GetObject",
 13         "s3:PutObject"
 14      ],
 15       "Resource": "arn:aws:s3::::soniyamishra10bucket/*"
 16     },
 17     {
 18       "Sid": "Stmt1634203670252",
 19       "Effect": "Allow",
 20       "Principal": "*",
 21       "Action": "s3:GetObject",
 22       "Resource": "arn:aws:s3::::soniyamishra10bucket/*"
 23     }
 24   ]
 25 } ]
```

⌚ Successfully edited bucket policy.

Amazon S3 > soniyamishra10bucket

soniyamishra10bucket [Info](#)

Publicly accessible

Objects Properties Permissions Metrics Management Access Points

Permissions overview

Access

⚠️ 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 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 changes, review the individual settings below to suit your specific needs.

Edit

Block **all** public access

A screenshot of a web browser window. The address bar shows the URL: `soniyamishra10bucket.s3.us-west-2.amazonaws.com/sample-file.txt`. Below the address bar is a toolbar with several icons: Apps, Managed bookmarks, India Intranet Hom..., AWS Management..., What is a core char..., and Applied eC: MuleSo... The main content area of the browser displays the following text:

```
This sample text file is used to illustrate the use of versioning in an Amazon S3 bucket.  
Make it a great day!
```

E) Explore versioning

Introduction to CloudWatch

Lab Steps

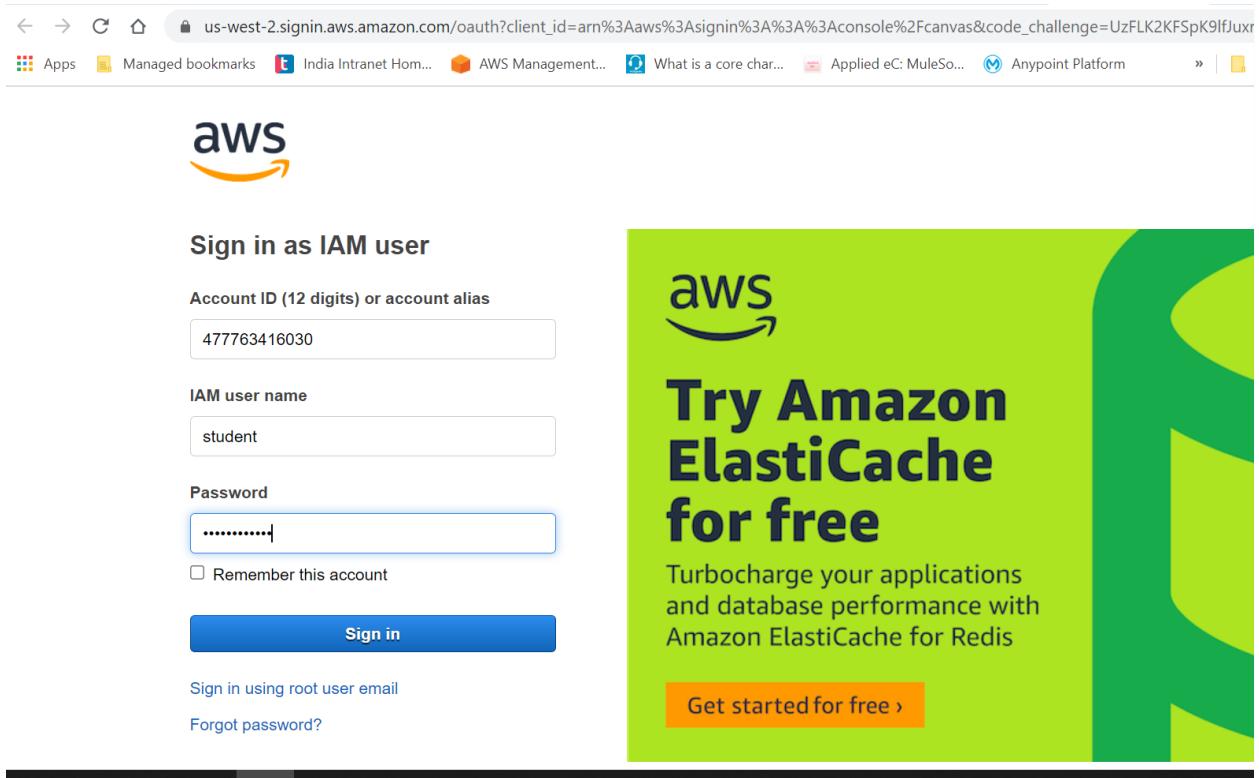
1. Logging in to the Amazon Web Services Console

1. To start the lab experience, open the Amazon Console by clicking the **Open Environment** button in the upper-left corner of the lab:

The screenshot shows a Cloud Academy lab environment. At the top, there's a navigation bar with icons for back, forward, and home, followed by the URL: cloudacademy.com/lab/introduction-to-cloudwatch/log-in-to-the-amazon-web-service-console/. Below the URL are links for 'Managed bookmarks', 'India Intranet Hom...', 'AWS Management...', 'What is a core char...', and 'Applied eC: MuleSc...'. The main content area has a green header bar with the title 'Logging in to the Amazon Web Services Console'. On the left, there's a sidebar with a progress bar showing '100% Setup completed' and a section titled 'Credentials' containing fields for 'Account ID', 'Username', and 'Password', each with a 'Copy' button. To the right, there's an 'Introduction' section with text about the lab experience and a preview of the AWS Management Console interface.

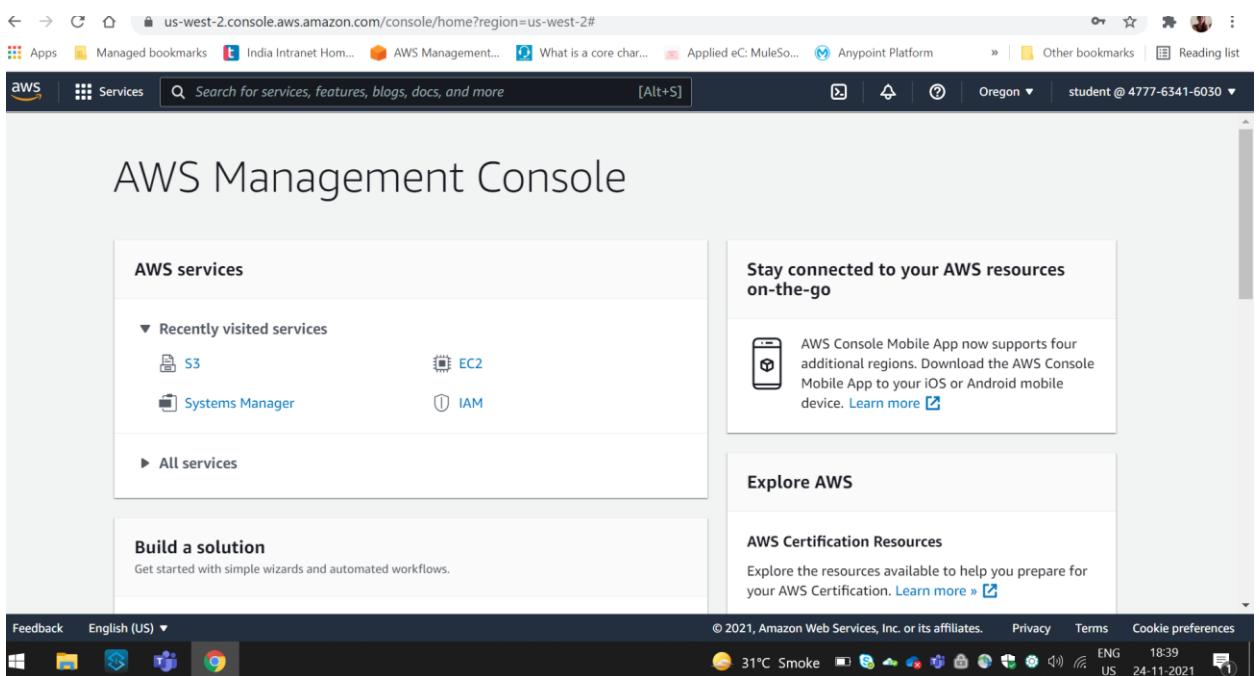
2. Enter the following credentials created just for your lab session, and click **Sign in**:

- **Account ID or alias:** 477763416030
- **IAM user name:** *student*
- **Password:** *Ca1_cJ4EaIaL*



The screenshot shows the AWS sign-in page for an IAM user. The URL is https://us-west-2.siginin.aws.amazon.com/oauth?client_id=arn%3Aaws%3Asignin%3A%3A%3Aconsole%2Fcanvas&code_challenge=UzFLK2KFSpK9lfJuxr. The page has a "Sign in as IAM user" header. It includes fields for "Account ID (12 digits) or account alias" (477763416030), "IAM user name" (student), and "Password" (redacted). There is a "Remember this account" checkbox and a "Sign in" button. Below the form are links for "Sign in using root user email" and "Forgot password?". To the right, there is a green promotional banner for Amazon ElastiCache, which says "Try Amazon ElastiCache for free" and "Turbocharge your applications and database performance with Amazon ElastiCache for Redis". A "Get started for free >" button is also present.

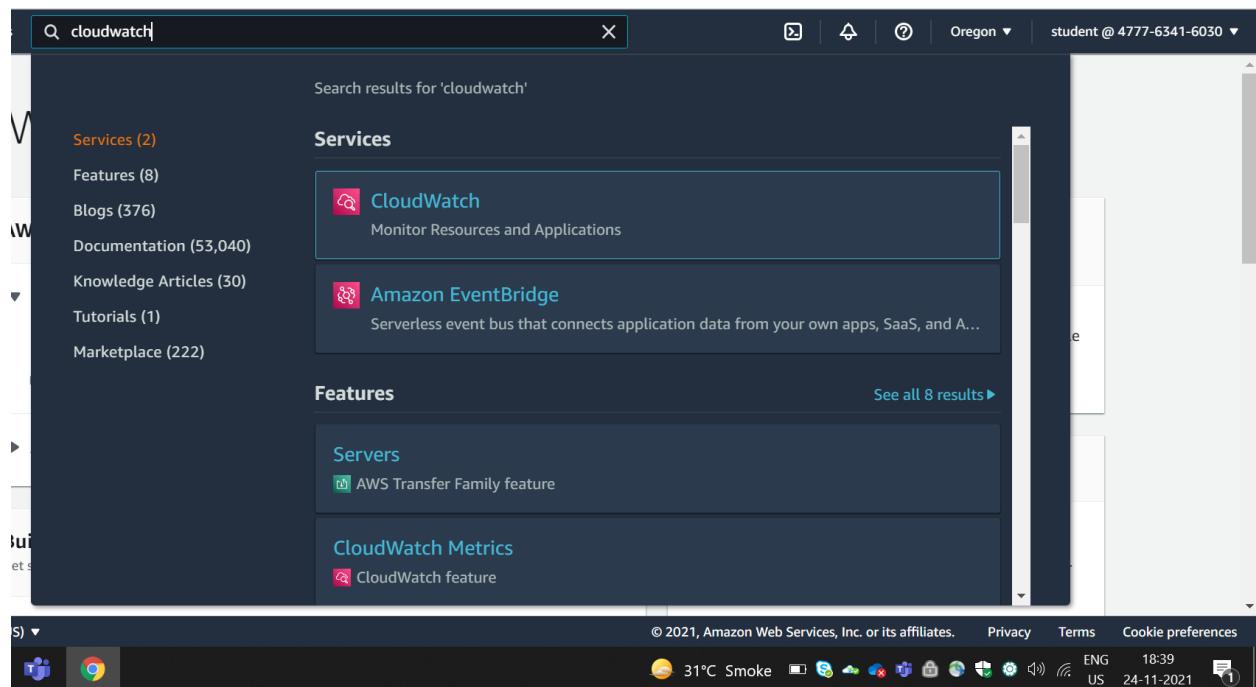
Select the **US West (Oregon)** us-west-2 region using the upper-right drop-down menu on the AWS Management Console:



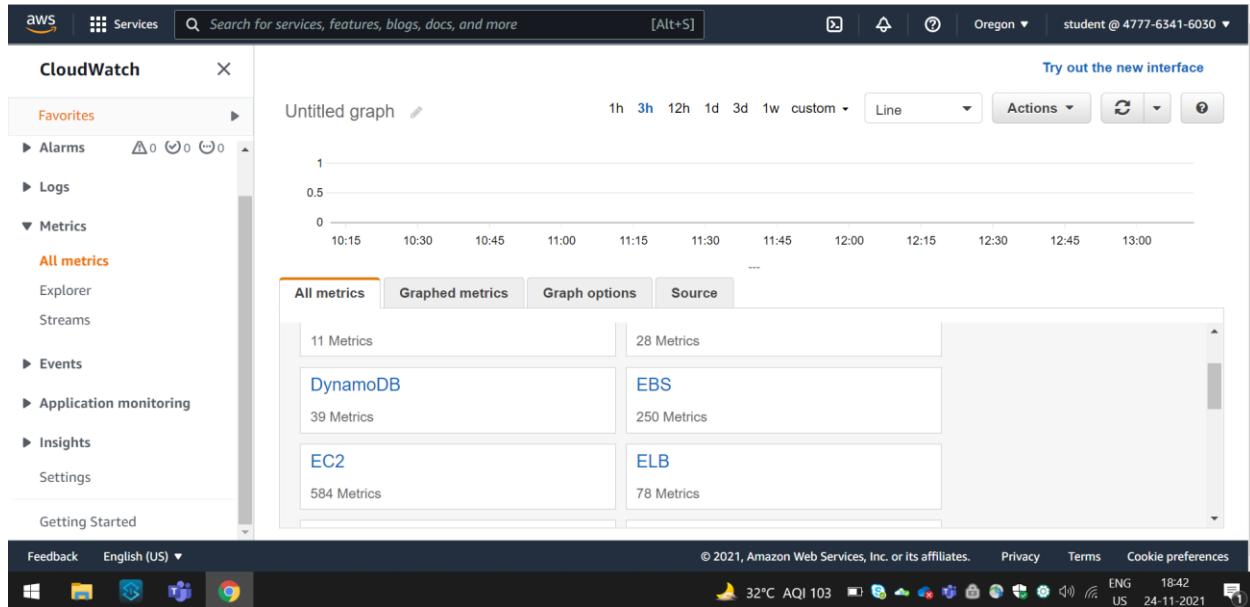
The screenshot shows the AWS Management Console home page for the us-west-2 region. The URL is <https://us-west-2.console.aws.amazon.com/console/home?region=us-west-2#>. The top navigation bar includes links for "Services", "Search for services, features, blogs, docs, and more", and a search bar. The main content area features the "AWS Management Console" logo and sections for "AWS services", "Build a solution", and "Stay connected to your AWS resources on-the-go". The "AWS services" section shows recently visited services like S3, EC2, Systems Manager, and IAM. The "Build a solution" section offers simple wizards and automated workflows. The "Stay connected" section promotes the AWS Console Mobile App. At the bottom, there are links for "Feedback", "English (US)", "Privacy", "Terms", and "Cookie preferences". The status bar at the bottom right shows the date (24-11-2021), time (18:39), and system information (ENG US).

2. Explore CloudWatch

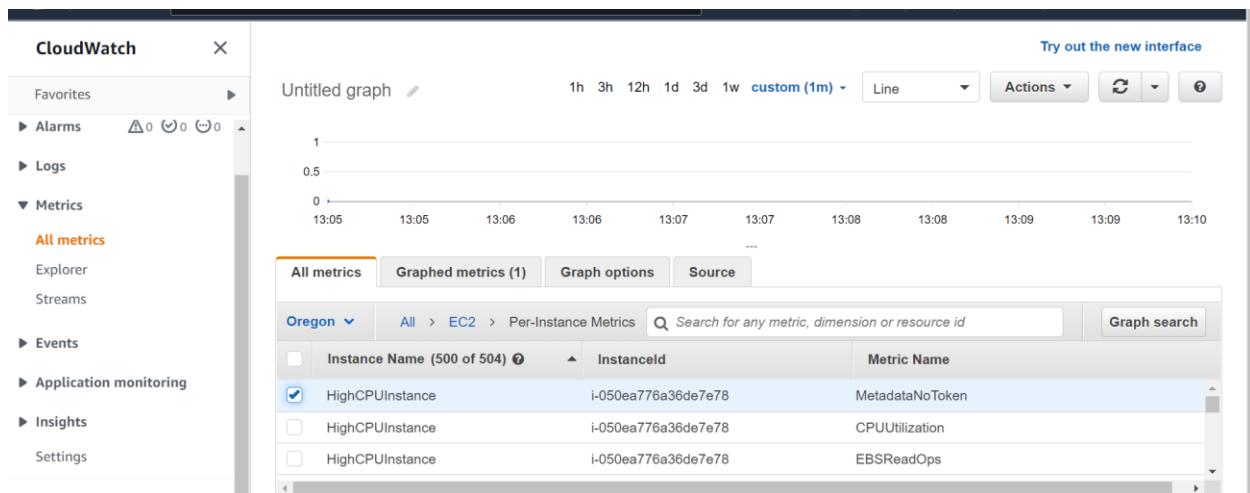
In the AWS Management Console search bar, enter **CloudWatch**, and click the **CloudWatch** result under **Services**:



Click **Metrics > All metrics** in the left navigation pane

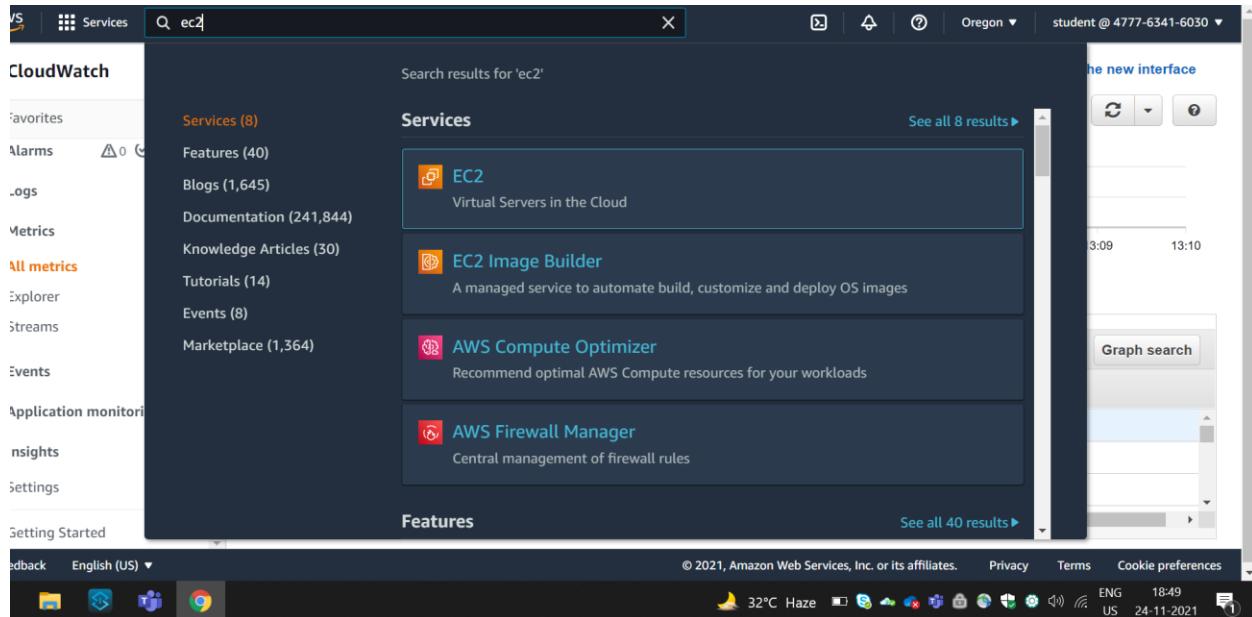


Spend a few minutes to explore what metrics, and namespaces look like in the CloudWatch console

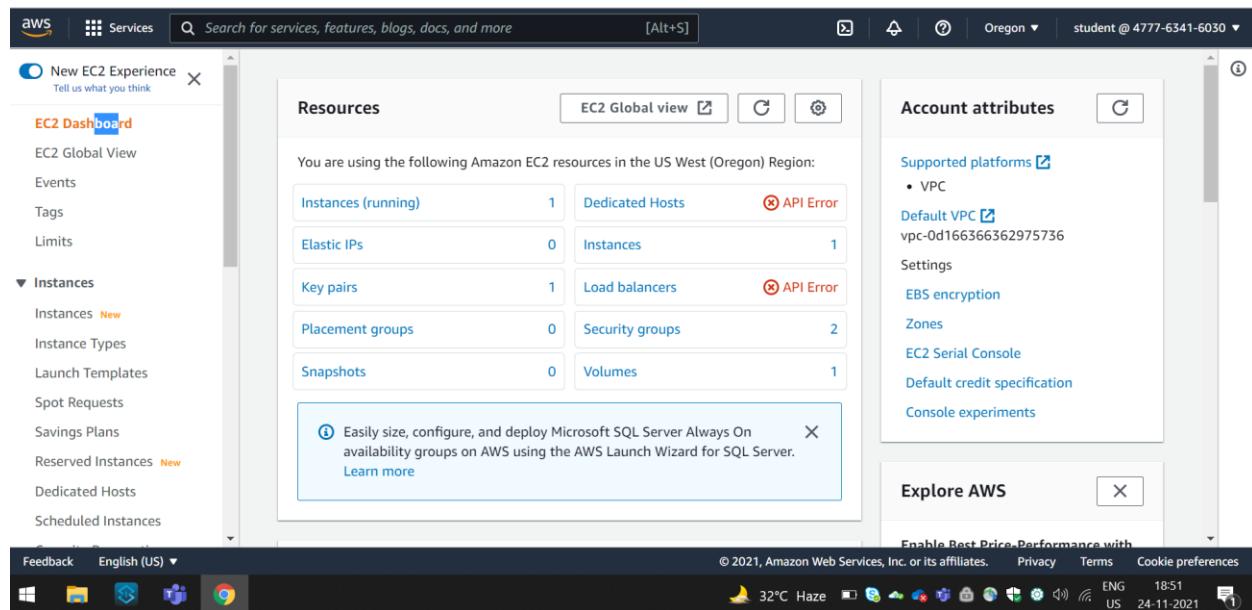


3. Monitoring EC2 Instances

In the AWS Management Console search bar, enter *EC2*, and click the *EC2* result under Services:



2. Click on Running Instances :



Select the box near the instance name. A wealth of instance information is displayed in the **Details** tab:

3. Select the box near the instance name

The screenshot shows the AWS EC2 Instances page. The left sidebar has 'Instances' expanded, with 'Instances New' selected. The main area displays one instance: 'HighCPUInsta...' (Instance ID: i-050ea776a36de7e78). The instance is listed as 'Running' (Status check: 2/2 checks passed), type m5.large, and alarm status: No alarms. The 'Actions' dropdown menu is open, showing options like 'Stop', 'Start', 'Reboot', 'Replace', and 'Delete'.

4. Switch to the **Monitoring** tab and take a look at the standard metrics:

The screenshot shows the same EC2 Instances page, but the 'Monitoring' tab is now selected in the navigation bar. Below the tabs, there's a 'Manage detailed monitoring' button and a time range selector (1h, 3h, 12h, 1d, 3d, 1w, Custom). Underneath, four metrics are displayed: 'CPU utilization (...)', 'Status check fail...', 'Status check fail...', and 'Status c...'. At the bottom of the page, there are links for 'Privacy', 'Terms', and 'Cookie preferences', along with a copyright notice: '© 2021, Amazon Web Services, Inc. or its affiliates.'

5. With the running instance selected, click the **Storage** tab. Scroll down and click on the **Volume Id** (lower right):

Instance: i-050ea776a36de7e78 (HighCPUInstance)

Volume ID	Device name	Volume size (GiB)	Attachment status	Attachment time	Encrypt
vol-0ec1ce0dfb108fb8c	/dev/xvda	8	Attached	Wed Nov 24 2021 18:31:07...	No

Recent root volume replacement tasks

Replace root volume

Click on the **Monitoring** tab to see the metrics for this EBS volume:

4. Install the EC2 Monitoring Scripts

In the AWS Management Console search bar, enter *EC2*, and click the EC2 result under Services:

From the Dashboard click on **Launch Instance**:

On Step 1 of the wizard, select Amazon Linux 2 AMI:

On Step 2, select **t2.micro** as the **Instance Type**, then click **Next: Configure Instance Details**.

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance families ▾ Current generation ▾ Show/Hide Columns

Currently selected: t2.micro (- ECUs, 1 vCPUs, 2.5 GHz, ~ 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	t2	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	t2	t2.small	1	2	EBS only	-	Low to Moderate	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

Feedback English (US) ▾ © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 32°C Haze ENG 19:04 US 24-11-2021

6. Click on **IAM role** and select the IAM role provided. It will have a name that looks similar to `cloudacademylabs-`

Check the **Enable CloudWatch detailed monitoring** box:

Configure Instance Details

Domain join directory No directory Create new directory

IAM role cloudacademylabs-EC2MonitoringRole-MN48OLSDS Create new IAM role

Shutdown behavior Stop

Stop - Hibernate behavior Enable hibernation as an additional stop behavior

Termination protection Protect against accidental termination

Monitoring **Enable CloudWatch detailed monitoring** Additional charges apply.

Tenancy Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.

Elastic Inference Add an Elastic Inference accelerator Additional charges apply.

Cancel Previous Review and Launch Next: Add Storage

English (US) ▾ © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 32°C Haze ENG 19:08 US 24-11-2021

. Copy and paste the following bash script code in the **User data (As text)** field:

Configure Instance Details

File systems [Add file system](#) [Create new file system](#)

Selected Details

Enclave [i](#) Enable

Metadata accessible [i](#) Enabled

Metadata version [i](#) V1 and V2 (token optional)

Token response hop limit [i](#) 1

User data [i](#) As text As file Input is already base64 encoded

```
#!/bin/bash
yum install -y perl-Switch perl-DateTime perl-Sys-Syslog perl-LWP-Protocol-
https perl-Digest-SHA.x86_64
wget http://aws-
cloudwatch.s3.amazonaws.com/downloads/CloudWatchMonitoringScripts-
1.2.2.zip
```

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

English (US) © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 32°C Haze ENG US 19:09 24-11-2021

9. Click **Review and Launch**, then **Launch**. A dialog box will appear asking for a Key Pair. Select **Proceed without a key pair**, mark the "**I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI**" checkbox and finally click on **Launch Instances**.

Step 7: Review Instance Launch

AMI Details [Edit AMI](#)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type - ami-0142f6ace1c558c7d
Free tier eligible Amazon Linux 2 comes with five years support. It provides Linux kernel 5.10 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is n...
Root Device Type: ebs Virtualization type: hvm

Instance Type [Edit instance type](#)

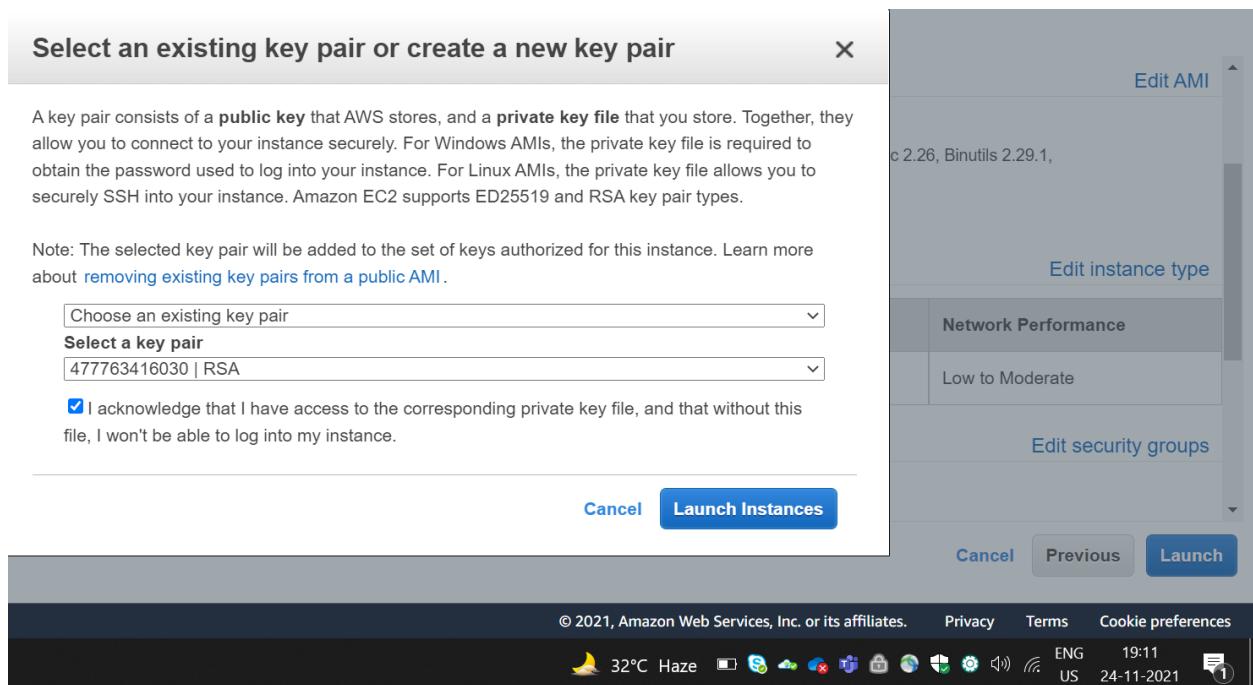
Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	-	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security group name: launch-wizard-1

[Cancel](#) [Previous](#) [Launch](#)

Feedback English (US) © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 32°C Haze ENG 19:11



Our Instances

ing, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and you stop or terminate your instances.

monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your instances.

Helpful resources to get you started

- [Amazon Linux instance](#)
- [Amazon EC2: User Guide](#)
- [Amazon Usage Tier](#)
- [Amazon EC2: Discussion Forum](#)

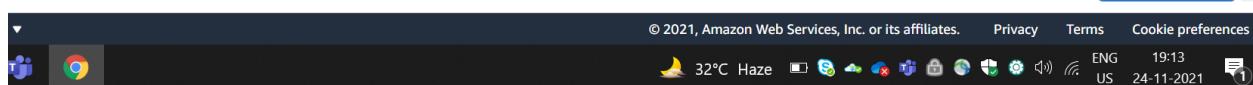
Before launching you can also

alarms to be notified when these instances fail status checks. (Additional charges may apply)

[Additional EBS volumes](#) (Additional charges may apply)

ips

[View Instances](#)



Click **View Instances**. Notice the **Name** for the new instance is blank by default. Although not mandatory, it is helpful to have a name. Move your mouse into the blank space in the **Name** column. It turns to an *edit pencil*. Use the pencil to change your **Instance Name** to *Monitoring Scripts*:

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
HighCPUInsta...	i-050ea776a36de7e78	Running	m5.large	2/2 checks passed	No alarms
<input checked="" type="checkbox"/> Edit Name		Running	t2.micro	Initializing	No alarms

Cancel Save

Instance: i-0e9b766753a940b60

English (US) © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 32°C Haze ENG US 19:13 24-11-2021

Instances (1/2) Info

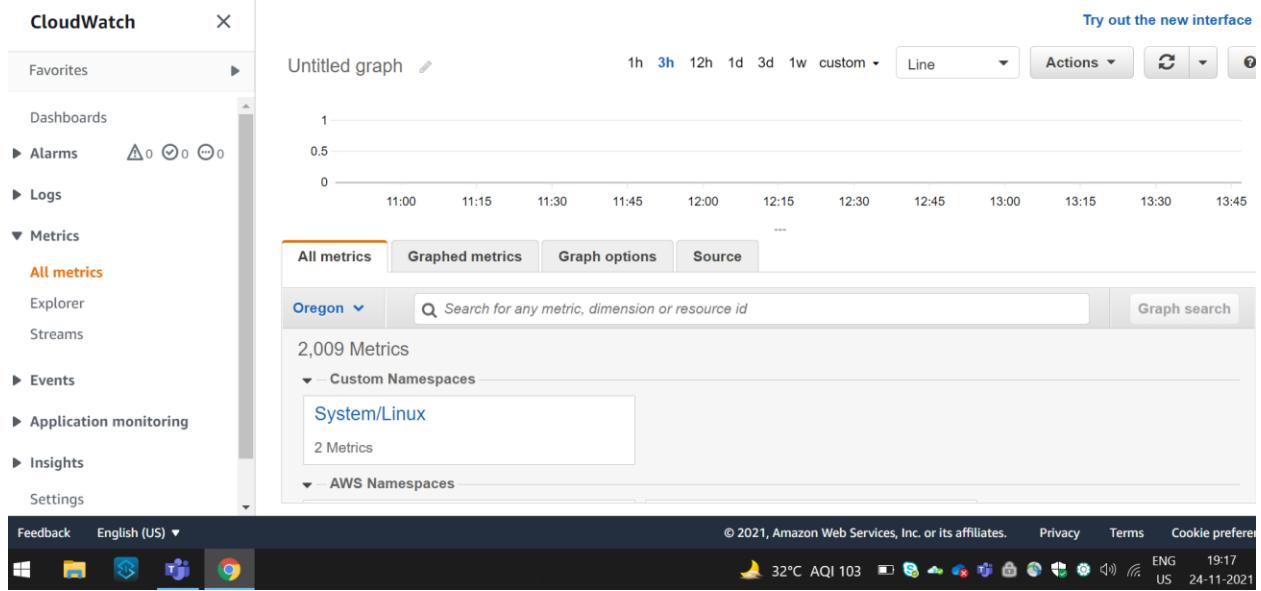
Name	Instance ID	Instance state	Instance type	Status check	Alarm status
HighCPUInsta...	i-050ea776a36de7e78	Running	m5.large	2/2 checks passed	No alarms
<input checked="" type="checkbox"/> Monitoring Scr...	i-0e9b766753a940b60	Running	t2.micro	Initializing	No alarms

Cancel Save

Instance: i-0e9b766753a940b60 (Monitoring Scripts)

© 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 32°C Haze ENG US 19:15 24-11-2021

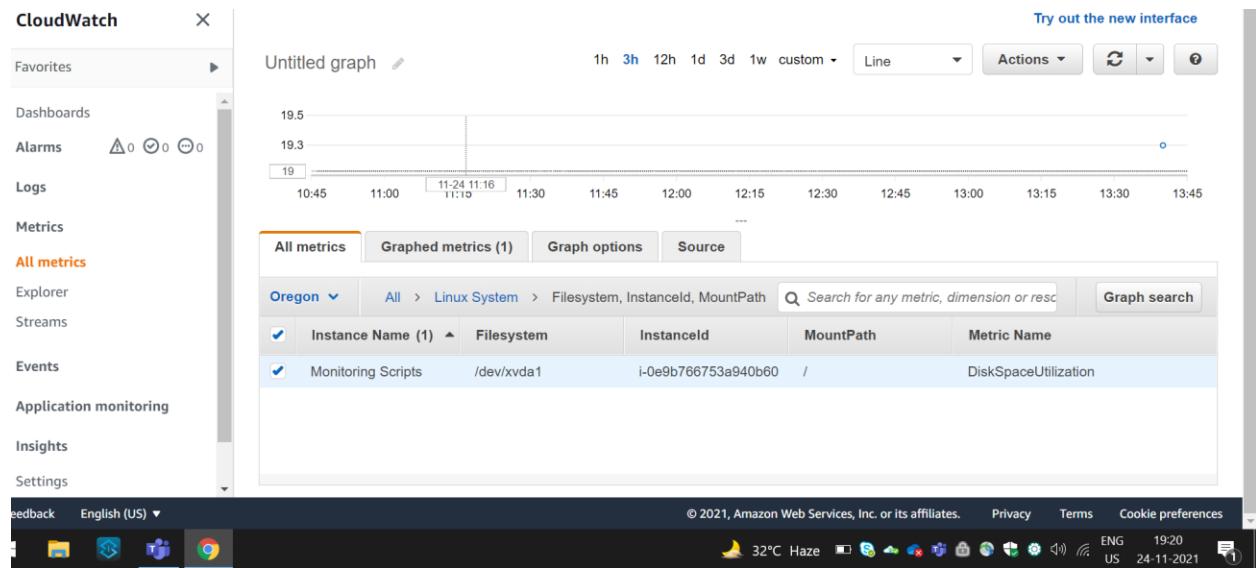
Return to **Services > CloudWatch > Metrics**. Notice that there is a new **Custom Namespace** called **Linux System**:



Click on the new **Linux System** namespace:

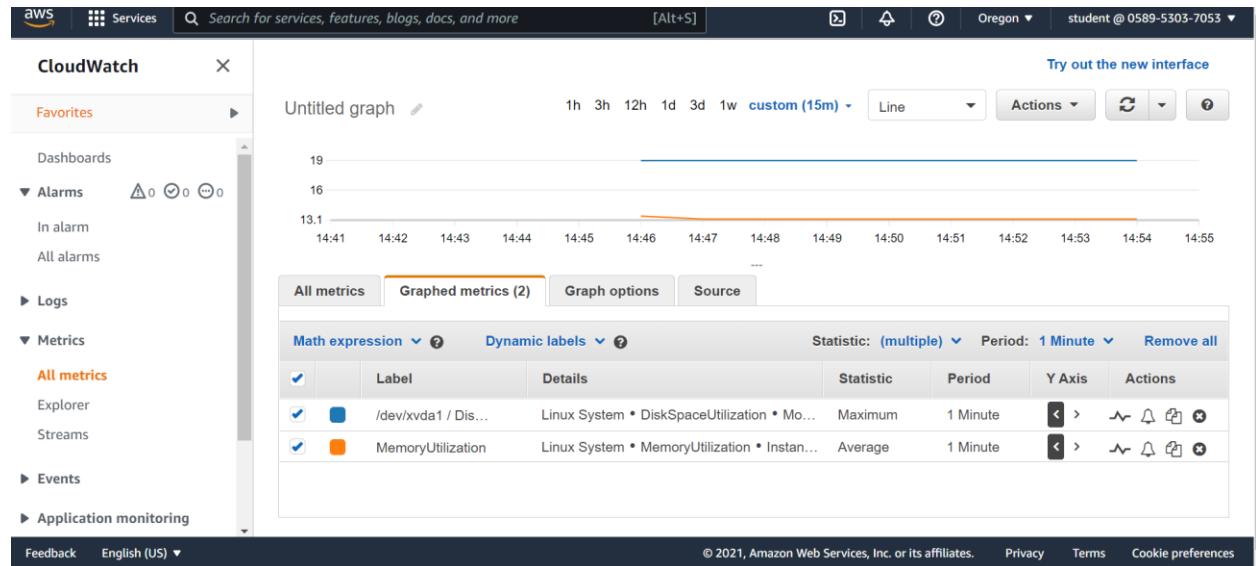
Click the metric on the left (**Filesystem...**), then select the checkbox so the first metric is graphed.

15. Click **Linux System**, so the **Metrics** path is **All > Linux System** again. Now select the metric on the right (**InstanceId**) and select its checkbox as well.



Click the **custom** graph period drop-down above the graph display area and select **15 Minutes**:

Select the **Period** drop-down column menu for each metric in the lower **Graphed metrics** tab and choose **1 Minute**:



5. Creating Your First CloudWatch Alarm

Go to the CloudWatch console and click on Alarms in the left pane:

The screenshot shows the AWS CloudWatch Alarms page. On the left, there's a navigation sidebar with 'Alarms' selected. The main area displays a table titled 'Alarms (0)' with columns for Name, State, Last state update, and Conditions. A message says 'No alarms' and 'No alarms to display'. At the bottom right of the table is a 'Create alarm' button.

Click **Create Alarm** and click **Select metric**. Select the **EC2** namespace then select **Per-Instance Metrics**:

The screenshot shows the 'Specify metric and conditions' step of the CloudWatch Create alarm wizard. On the left, a sidebar lists steps: Step 1 (Specify metric and conditions), Step 2 (Configure actions), Step 3 (Add name and description), and Step 4 (Preview and create). The main area has sections for 'Metric' and 'Graph'. Under 'Metric', there's a 'Select metric' button. At the bottom right are 'Cancel' and 'Next' buttons. The status bar at the bottom indicates it's step 1 of 4.

Select metric

Untitled graph

1h 3h 12h 1d 3d 1w Custom Line

AWS Namespaces

ApiGateway	11	CodeBuild	28	DynamoDB	39
EBS	259	EC2	608	ELB	78

Select a single metric to continue

Select metric

Metrics (608)

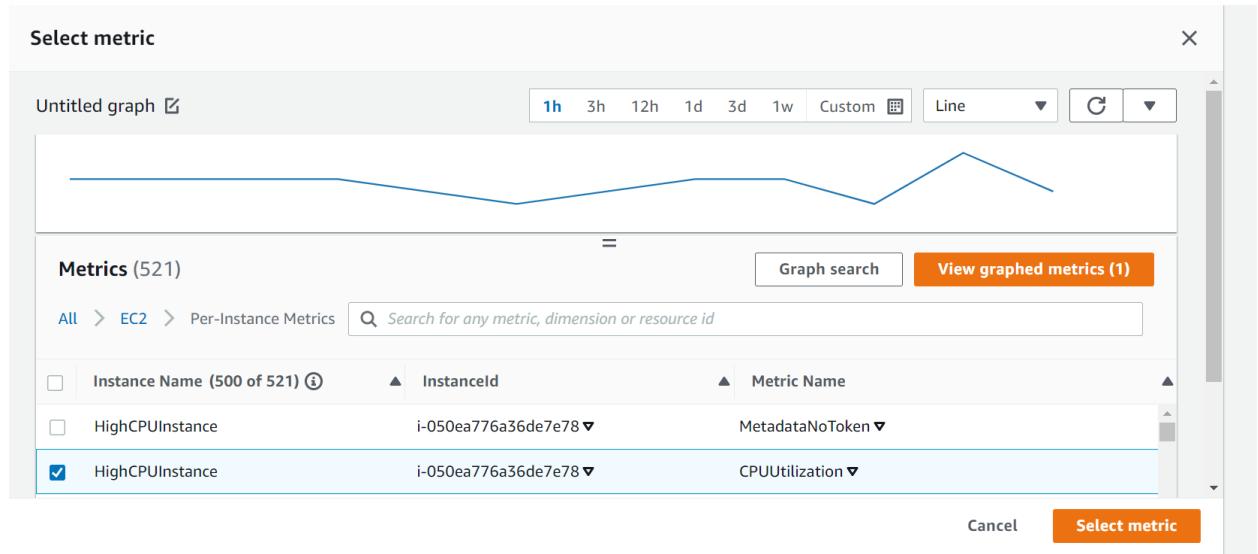
All > EC2 Search for any metric, dimension or resource id

By Auto Scaling Group	34	By Image (AMI) Id	26	Per-Instance Metrics	521
Aggregated by Instance Type	15	Across All Instances	12		

Select a single metric to continue

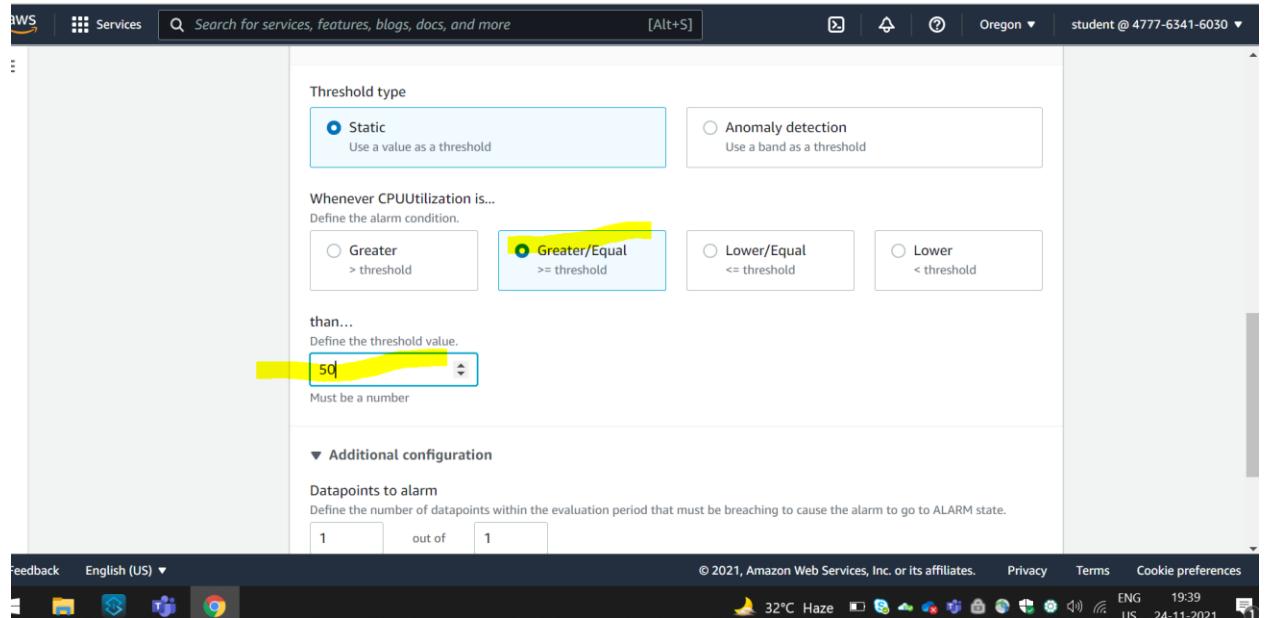
English (US) ▾ © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 32°C Haze ENG US 19:32 24-11-2021

Click **Per-instance metrics** and select the **CPUUtilization Metric Name** for the running **HighCPUInstance**



- Whenever High CPU is...: Greater/Equal
- Than...:50

Click Next:



Fill the form as described

- Whenever this alarm state is...: in Alarm
- Select an SNS topic: Create new topic

Insert a valid e-mail and click on Create topic.

The screenshot shows the configuration of an AWS CloudWatch alarm. At the top, there are three status options: **In alarm** (selected), **OK**, and **Insufficient data**. Below these, the user is prompted to "Select an SNS topic" and defines the topic name as "Default_CloudWatch_Alarms_Topic". The user has also specified email endpoints: "mishrasoniya1999@gmail.com" and "user1@example.com, user2@example.com". A "Create topic" button is visible. The footer includes copyright information, links to Privacy, Terms, and Cookie preferences, and a system status bar showing weather (32°C Haze), system icons, and the date/time (ENG US 24-11-2021).

7. Click **Next** and fill the form as described

- **Define a unique name:** High CPU
- **Alarm description:** When CPU utilization $\geq 50\%$

Click **Next**.

CloudWatch > Alarms > Create alarm

Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Add name and description

Name and description

Alarm name: High CPU

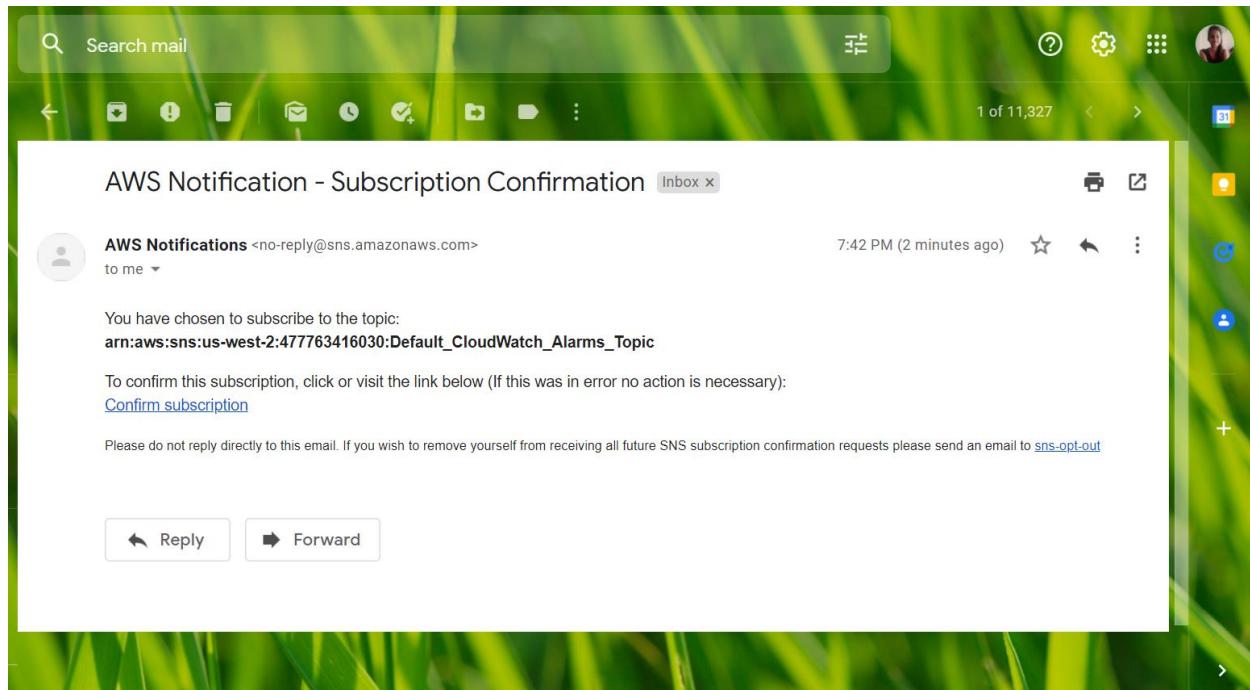
Alarm description - optional:
When CPU utilization >= 50%

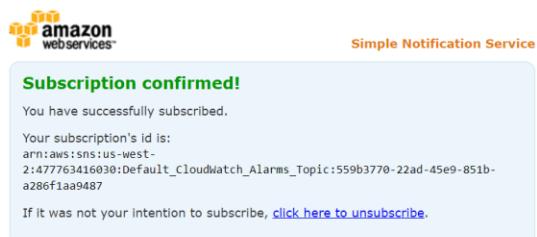
Up to 1024 characters (28/1024)

Cancel Previous Next

Click **Create Alarm** when ready.

Check for an email from **AWS Notifications**. Open up the email and click the **Confirm subscription** link:





You should be put to the **Alarm** page:

Name	State	Last state update	Conditions
High CPU	In alarm	2021-11-24 19:45:43	CPUUtilization >= 50 for 1 datapoints within 5 minutes

. Click the **Alarm**. You can see very useful information about the alarm itself. In the **Details** tab there is a general overview of the alarm, and in the **History** tab you can see up to the last 50 states of the alarm:

The screenshot shows the AWS CloudWatch Alarms interface. On the left, a sidebar lists 'Alarms (1)'. The main panel displays a single alarm named 'High CPU' with the following details:

Setting	Value
Name	High CPU
Type	Metric alarm
Description	When CPU utilization >= 50%
Namespace	AWS/EC2
Metric name	CPUUtilization
Threshold	CPUUtilization >= 50 for 1 datapoints within 5 minutes
Last change	2021-11-24 14:15:43
Actions	Actions enabled
Datapoints to alarm	1 out of 1
Missing data treatment	Discard

At the bottom, there is a footer with copyright information and navigation links.

The screenshot shows the AWS CloudWatch Alarms History page for the 'High CPU' alarm. The sidebar on the left is identical to the previous screenshot. The main panel shows the history of the alarm's state changes:

Date	Type	Description
2021-11-24 14:15:43	Action	Successfully executed action arn:aws:sns:us-west-2:477763416030:Default_CloudWatch_Alarms_Topic
2021-11-24 14:15:43	State update	Alarm updated from Insufficient data to In alarm
2021-11-24 14:15:14	Configuration update	Alarm "High CPU" created

6. Create an Alarm using the EC2 console

1. Navigate to Services > EC2 > Instances.

Select the **Monitoring Scripts** instance, then switch to the **Status Checks** tab:

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
HighCPUInsta...	i-050ea776a36de7e78	Running	m5.large	2/2 checks passed	1/1 in al +
Monitoring Scr...	i-0e9b766753a940b60	Running	t2.micro	2/2 checks passed	No alarms +

Instance: i-0e9b766753a940b60 (Monitoring Scripts)

Status checks Info

Status checks detect problems that may impair i-0e9b766753a940b60 (Monitoring Scripts) from running your applications.

Actions ▾

System status checks	Instance status checks
System reachability check passed	Instance reachability check passed

c2/v2/home?region=us-west-2# © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 32°C Haze ENG US 19:52 24-11-2021 1

. Click **Actions > Create Status Check Alarm**. A **Create Alarm** dialog is presented so you can configure the details of the alarm:

Instances (1/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
HighCPUInsta...	i-050ea776a36de7e78	Running	m5.large	2/2 checks passed	1/1 in al +
Monitoring Scr...	i-0e9b766753a940b60	Running	t2.micro	2/2 checks passed	No alarms +

Instance: i-0e9b766753a940b60 (Monitoring Scripts)

Status checks Info

Status checks detect problems that may impair i-0e9b766753a940b60 (Monitoring Scripts) from running your applications.

Actions ▾

Create status check alarm
Report Instance status

System status checks	Instance status checks
System reachability check passed	Instance reachability check passed

c2/v2/home?region=us-west-2# © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 32°C AQI 108 ENG US 19:53 24-11-2021 1

For the **Alarm notification**, select the SNS topic name and valid email you set up before.

The screenshot shows the 'Manage CloudWatch alarms' page. At the top, there's a heading 'Add or edit alarm' with a 'Create an alarm' button highlighted. Below it is a search bar for finding existing alarms. Under 'Alarm notification', a dropdown menu is open, showing 'Default_CloudWatch_Alarms_Topic' selected. The bottom of the screen shows the standard AWS navigation bar with various icons and user information.

Return to the **Alarms** page in the CloudWatch console.

The screenshot shows the 'Alarms' page in the CloudWatch console. A green banner at the top indicates a new CloudWatch alarm has been created. The main table displays two instances: 'Monitoring Scr...' and 'HighCPUInsta...', both of which are running and have passed 2/2 checks. The bottom of the screen shows the standard AWS navigation bar.

The screenshot shows the AWS CloudWatch Alarms interface. On the left, a sidebar lists various monitoring categories like Dashboards, Alarms, Metrics, and Events. The 'Alarms' section is expanded, showing 0 pending, 1 active, and 1 in alarm. The 'In alarm' section lists 'All alarms'. The main pane displays two alarms: 'awsec2-i-Oa166261ff5089b6' (OK) and 'High CPU' (Insufficient data). The 'High CPU' alarm has a status message: 'StatusCheckFailed >= 0.99 for 1 datapoints within 5 minutes'. The bottom of the screen shows the AWS footer with copyright information, privacy terms, and cookie preferences, along with system status icons.

Select the **High CPU** alarm and then **Actions > Edit**:

- . Click on **Next** and click on **Add EC2 action**. Select **Reboot this instance**.

The screenshot shows the 'Edit alarm' configuration page. It features three tabs: 'Auto Scaling action', 'EC2 action', and 'Systems Manager action'.

- Auto Scaling action:** Contains a button 'Add Auto Scaling action'.
- EC2 action:** Contains a button 'Add EC2 action'.
- Systems Manager action:** Contains a button 'Add Systems Manager action'. Below it, a note states: 'This action will create an Incident or OpsItem in Systems Manager when the alarm is **In alarm** state.'

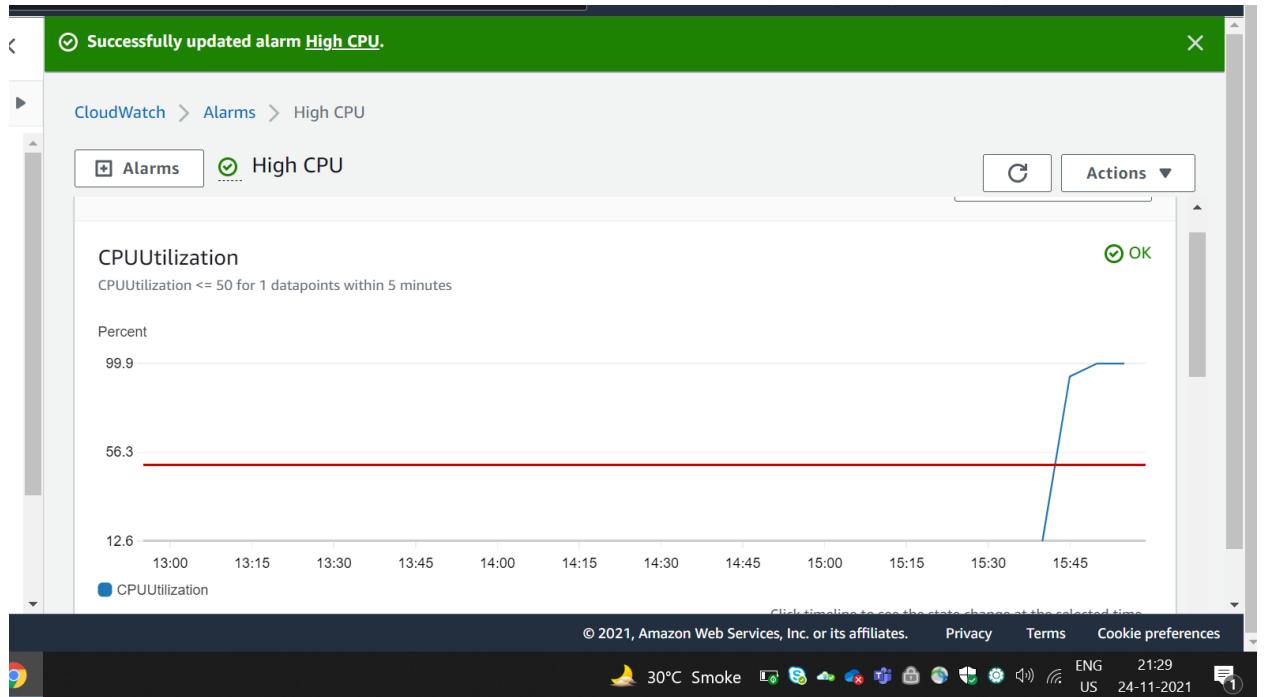
At the bottom, there are navigation buttons: 'Cancel', 'Previous', 'Next', and an orange 'Update alarm' button.

Select the **High CPU Alarm** and choose **Actions > Modify**. Simply toggle the relationship from \geq to \leq . Save the changes and refresh the page to ensure the alarm has

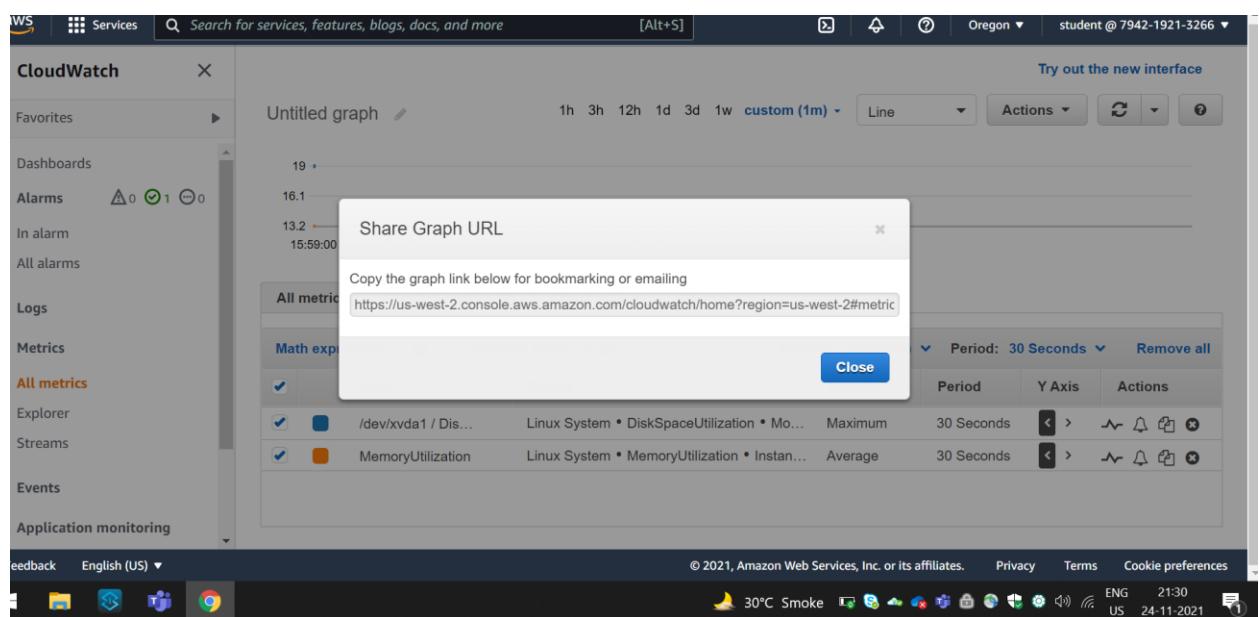
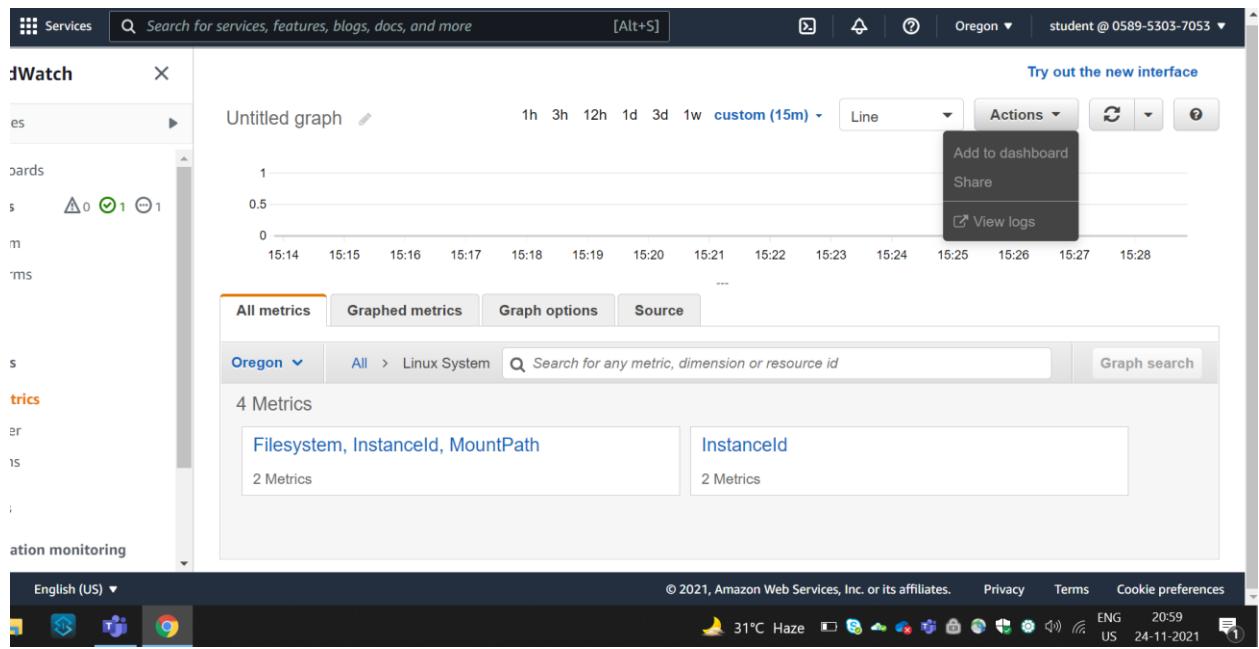
transitioned to the **OK** state. Then toggle the condition back to \geq and save the alarm to have it transition to the **ALARM** state.

Pend a few minutes in the **Instances** page of the EC2 console and watch

CloudWatch reboot the instance when the **Alarm Status** changes to **ALARM**.



7. Sharing CloudWatch Metrics with others



Practical No. 4

Introduction to Amazon API Gateway

Aim: A) Create a Lambda Function

B) Test the Lambda function Conclusion

The screenshot shows the AWS Management Console home page for the us-west-2 region. The navigation bar at the top includes links for various services like My Drive, AWS, Pract, Qwik, and AWS. The main content area has a sidebar titled 'Recently visited services' and a 'Services' section with a search bar. The 'All services' section is expanded, showing categories like Compute, Machine Learning, and Containers, each listing several AWS services. To the right, there are promotional boxes for the AWS Console Mobile App and AWS Cloud Training, followed by sections for Free AWS Training and AWS Certification.

Click on lambda

The screenshot shows the AWS Management Console home page. At the top, there is a navigation bar with tabs for various services like Inbox, My Drive, AWS Practice, AWS Pro, Qwiklabs, Introduction, and AWS Mobile. Below the navigation bar is a search bar and a dropdown for the region set to Oregon. A user profile is also visible.

The main content area has a sidebar on the left with sections for "Recently visited services" and "All services". Under "All services", there are two columns: "Compute" and "Machine Learning".

Compute Services:

- EC2
- Lightsail
- [Lambda](#)
- Batch
- Elastic Beanstalk
- Serverless Application Repository
- AWS Outposts
- EC2 Image Builder
- AWS App Runner

Machine Learning Services:

- Amazon SageMaker
- Amazon Augmented AI
- Amazon CodeGuru
- Amazon DevOps Guru
- Amazon Comprehend
- Amazon Forecast
- Amazon Fraud Detector
- Amazon Kendra
- Amazon Lex
- Amazon Personalize
- Amazon Polly
- Amazon Rekognition
- Amazon Textract
- Amazon Transcribe
- Amazon Translate
- AWS DeepComposer

On the right side of the page, there is a promotional box for the AWS Console Mobile App, which now supports four additional regions. It includes a download link for iOS or Android devices.

Below the promotional box is a section titled "Explore AWS" with links to "AWS Cloud Training" and "Free AWS Training".

At the bottom of the page, there are links for "Feedback", "English (US)", "Privacy", "Terms", and "Cookie preferences". The browser's address bar shows the URL <https://us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2>. The taskbar at the bottom of the screen shows icons for File Explorer, Task View, Edge, File Explorer, Mail, Google Photos, and a system tray with a battery icon showing 10%.

The screenshot shows the AWS Lambda console interface. On the left, a sidebar menu includes options like Dashboard, Applications, Functions (which is selected), Additional resources, and Related AWS resources. The main content area is titled 'Functions (0)' and displays a table header with columns: Function name, Description, Package type, Runtime, and Code size. A message at the bottom of the table says 'There is no data to display.' The top navigation bar shows the URL 'us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2#/functions' and the AWS logo.

Click on create function

The screenshot shows the AWS Lambda 'Create function' wizard. At the top, there are four options: 'Author from scratch' (selected), 'Use a blueprint', 'Container image', and 'Browse serverless app repository'. Below this is a 'Basic information' section where the 'Function name' is set to 'myFunctionName'. The bottom of the screen includes a search bar, system icons, and a status bar showing '20°C', 'ENG', '09:02', and '02-12-2021'.

Choose one of the following options to create your function.

- Author from scratch Start with a simple Hello World example.
- Use a blueprint Build a Lambda application from sample code and configuration presets for common use cases.
- Container image Select a container image to deploy for your function.
- Browse serverless app repository Deploy a sample Lambda application from the AWS Serverless Application Repository.

Basic information

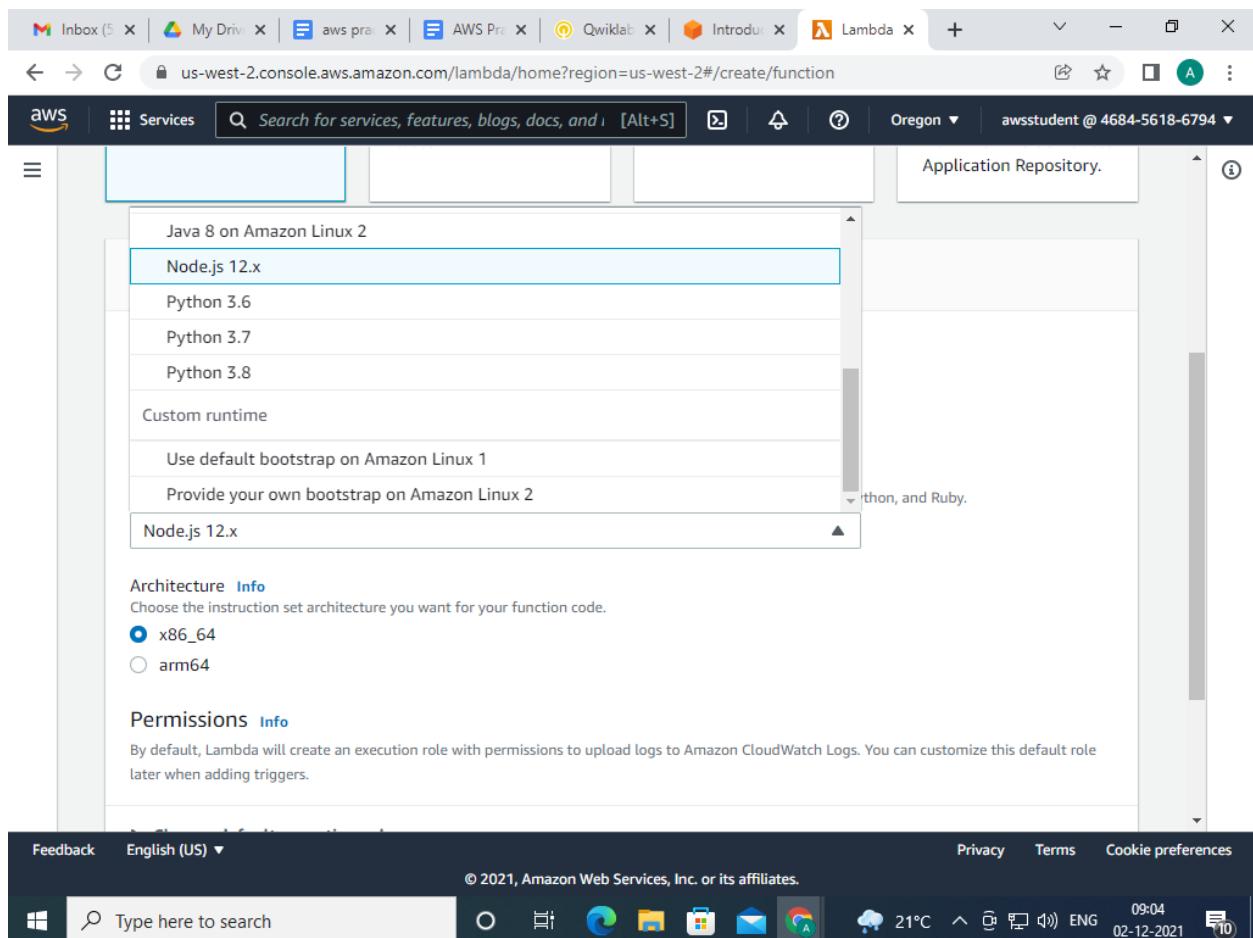
Function name
Enter a name that describes the purpose of your function.

Use only letters, numbers, hyphens, or underscores with no spaces.

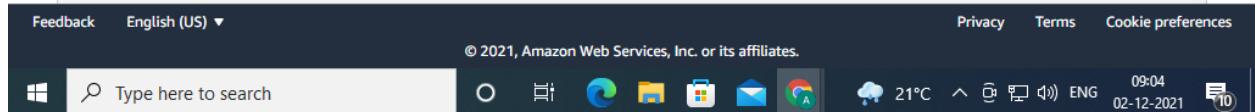
Feedback English (US) ▾ © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Type here to search

Function name:FAQ



The screenshot shows the AWS Lambda 'Create function' wizard. At the top, there's a navigation bar with tabs like 'Inbox', 'My Drive', 'aws pr...', 'AWS Pr...', 'Qwiklab', 'Introdu...', 'Lambda', and a '+' button. Below the navigation bar is a search bar and a dropdown for the region ('Oregon'). On the left, a sidebar lists runtime options: Python 3.8, Custom runtime, Use default bootstrap on Amazon Linux 1, Provide your own bootstrap on Amazon Linux 2, and Node.js 12.x. The 'Python 3.8' option is selected. The main content area has sections for 'Architecture' (Info) and 'Permissions'. Under 'Architecture', 'x86_64' is selected. Under 'Permissions', it says 'By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.' There are two expandable sections: 'Change default execution role' and 'Advanced settings'. At the bottom right are 'Cancel' and 'Create function' buttons.



The screenshot shows the AWS Lambda function creation interface. At the top, there's a navigation bar with tabs like 'Inbox', 'My Drive', 'aws pr...', 'AWS Pr...', 'Qwiklab', 'Introdu...', and 'Lambda'. The 'Lambda' tab is active. Below the navigation bar, the URL is 'us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2#/create/function'. The main content area starts with a language selection dropdown set to 'Node.js 12.x'. Under 'Architecture', 'x86_64' is selected. In the 'Permissions' section, it says 'By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.' A 'Change default execution role' section is expanded, showing three options: 'Create a new role with basic Lambda permissions' (unchecked), 'Use an existing role' (checked), and 'Create a new role from AWS policy templates' (unchecked). Below this, an 'Existing role' section is shown with a dropdown menu and a 'Create' button. The bottom of the page includes standard footer links for 'Feedback', 'English (US)', 'Privacy', 'Terms', and 'Cookie preferences', along with a search bar and system status indicators.

The screenshot shows the AWS Lambda 'Create function' wizard on the 'Permissions' step. The browser tab is 'Lambda' and the URL is 'us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2#/create/function'. The search bar contains 'Search for services, features, blogs, docs, and more [Alt+S]'. The top navigation bar includes 'Services' and a user dropdown 'awsstudent @ 4684-5618-6794'. The main content area shows a function named 'arm64' with the configuration 'arm64'. The 'Permissions' section is active, with a note that Lambda will create an execution role by default. It offers three options for the execution role:

- Create a new role with basic Lambda permissions
- Use an existing role
- Create a new role from AWS policy templates

The 'Use an existing role' option is selected. A dropdown menu shows a single entry: 'lambda-basic-execution'. Below the dropdown is a link to 'Advanced settings'. At the bottom right are 'Cancel' and 'Create function' buttons.

The screenshot shows the AWS Lambda 'Create function' wizard on the 'Permissions' step. The URL in the browser is us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2#/create/function. The page title is 'Lambda'. The left sidebar has 'Services' selected. The main content area is titled 'Permissions' with an 'Info' link. It states: 'By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.' Below this is a section titled '▼ Change default execution role'. It includes an 'Execution role' section with three options: 'Create a new role with basic Lambda permissions' (radio button), 'Use an existing role' (radio button, selected), and 'Create a new role from AWS policy templates'. An 'Existing role' section shows a dropdown menu set to 'lambda-basic-execution' with a 'View the lambda-basic-execution role on the IAM console.' link. There is also a '▼ Advanced settings' section. At the bottom right are 'Cancel' and 'Create function' buttons. The bottom of the screen shows a Windows taskbar with various icons and a system tray showing the date and time.

The screenshot shows the AWS Lambda console interface. At the top, there are tabs for Services, a search bar, and account information. Below the search bar, there are two buttons: '+ Add trigger' and '+ Add destination'. To the right, a panel displays the Function ARN: arn:aws:lambda:us-west-2:468456186794:function:FAQ, updated 33 seconds ago. Below this, there are tabs for Code, Test, Monitor, Configuration, Aliases, and Versions. The Code tab is selected, showing the 'Code source' section. The code editor displays the file index.js with the following content:

```
1 exports.handler = async (event) => {
2     // TODO implement
3     const response = {
4         statusCode: 200,
5         body: JSON.stringify('Hello from Lambda!'),
6     };
7     return response;
8 };
9
```

At the bottom of the screen, there is a Windows taskbar with a search bar, pinned icons for File Explorer, Edge, File Cabinet, Mail, and Google Chrome, and system status indicators.

Click on deploy

The screenshot shows the AWS Lambda console interface for a function named 'FAQ'. The top navigation bar includes tabs for 'Code', 'Test', 'Monitor', 'Configuration', 'Aliases', and 'Versions'. The 'Configuration' tab is currently selected. A modal window is open, prompting for 'Add trigger' or 'Add destination'. Below this, the 'Function ARN' is displayed as 'arn:aws:lambda:us-west-2:468456186794:function:FAQ'. The main area shows the code editor for 'index.js', which contains a JSON object with multiple questions and answers related to AWS Lambda functions. The code is as follows:

```
38  "q": "Why must AWS Lambda functions be stateless?",  
39  "a": "Keeping functions stateless enables AWS Lambda to rapidly launch as many  
40  }, {  
41  "q": "Can I use threads and processes in my AWS Lambda function code?",  
42  "a": "Yes. AWS Lambda allows you to use normal language and operating system fea  
43  }, {  
44  "q": "What restrictions apply to AWS Lambda function code?",  
45  "a": "Lambda attempts to impose few restrictions on normal language and operati  
46  }, {  
47  "q": "How do I create an AWS Lambda function using the Lambda console?",  
48  "a": "You can author the code for your function using the inline editor in the L  
49  }, {  
50  "q": "How do I create an AWS Lambda function using the Lambda CLI?",  
51  "a": "You can package the code (and any dependent libraries) as a ZIP and upload  
52  }, {
```

Click on configuration tab

The screenshot shows the AWS Lambda console interface. The top navigation bar includes tabs for Services, Search for services, features, blogs, docs, and more [Alt+S], Oregon, and awsstudent @ 4684-5618-6794. The main navigation path is Lambda > Functions > FAQ. The page title is FAQ. Action buttons include Throttle, Copy ARN, and Actions. A sidebar on the right has an info icon.

FAQ

Function overview Info

FAQ (0)

Layers (0)

+ Add trigger + Add destination

Description: -

Last modified: 3 minutes ago

Function ARN: arn:aws:lambda:us-west-2:468456186794:function:FAQ

Code | Test | Monitor | **Configuration** | Aliases | Versions

General configuration Info **Edit**

Feedback English (US) ▾ https://us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2# Amazon Web Services, Inc. or its affiliates.

Type here to search

Privacy Terms Cookie preferences

09:08 21°C ENG 02-12-2021 10

Then click on edit

The screenshot shows the AWS Lambda Configuration page for a function named 'FAQ'. The 'Configuration' tab is selected. On the left, a sidebar lists options: General configuration (selected), Triggers, Permissions, Destinations, Environment variables, Tags, and VPC. The main area displays 'General configuration' settings:

- Description: -
- Memory: 128 MB
- Timeout: 0 min 3 sec

A modal window titled 'AWS Compute Optimizer' is open, prompting the user to opt in for memory recommendations. The modal includes a 'View details' link and a close button ('X').

At the bottom of the page, there are links for Feedback, English (US) (language), Privacy, Terms, and Cookie preferences. The status bar at the bottom of the browser window shows the date (02-12-2021), time (09:09), and battery level (10%).

For description enter: Provide a random FAQ

Click on save

The screenshot shows the AWS Lambda console interface. The URL in the browser is `us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2#/functions/FAQ?newFunction=true&tab=...`. The top navigation bar includes tabs for Services, Search for services, features, blogs, docs, and more [Alt+S], Oregon, and awsstudent @ 4684-5618-6794. A green notification bar at the top says "Your changes have been saved." Below it, the breadcrumb navigation shows Lambda > Functions > FAQ. The main title is "FAQ". On the right, there are buttons for Throttle, Copy ARN, and Actions. Under the "Function overview" section, there is a thumbnail for the function icon labeled "FAQ", a "Layers (0)" section, and two buttons: "+ Add trigger" and "+ Add destination". To the right of these, the "Description" is listed as "Provide a random FAQ", "Last modified" as "2 minutes ago", and the "Function ARN" as "arn:aws:lambda:us-west-2:468456186794:function:FAQ". Below this, tabs for Code, Test, Monitor, Configuration (which is selected), Aliases, and Versions are visible. At the bottom, a dark footer bar includes links for Feedback, English (US) ▾, Privacy, Terms, and Cookie preferences, along with a search bar and system status indicators.

Click on Add Trigger

The screenshot shows the AWS Lambda console with the URL us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2#/add/trigger?focus=lambda&target=arn:aws:lambda:us-west-2:123456789012:function:my-lambda-function. The page title is "Add trigger". The "Trigger configuration" section contains a search bar with "Select a trigger" placeholder and a dropdown menu. The menu items are:

- API Gateway
- AWS IoT
- Alexa Skills Kit
- Alexa Smart Home
- Apache Kafka

The "API Gateway" item is selected and highlighted.

Then select api getway

Then create an api

The screenshot shows the AWS Lambda console with a modal dialog titled "Add relation". The dialog is for adding an API to a Lambda function. It includes fields for "API Name" (with "Create an API" selected), "HTTP API" (with "Create an HTTP API" selected), and "REST API" (with "Create a REST API" selected). There is also a "Security" section for configuring security mechanisms. At the bottom, there are "Cancel" and "Add" buttons.

Click on reset Api

The screenshot shows the AWS Lambda console with a modal dialog titled "Add relation". The dialog is for creating an API Gateway endpoint that triggers a Lambda function. The "REST API" option is selected under "API type". The "Security" section is collapsed. At the bottom right of the dialog are "Cancel" and "Add" buttons.

Add an API to your Lambda function to create an HTTP endpoint that invokes your function. API Gateway supports two types of RESTful APIs: HTTP APIs and REST APIs. [Learn more](#)

API
Create a new API or attach an existing one.

Create an API

API type

HTTP API
Create an HTTP API.

REST API
Create a REST API.

Security
Configure the security mechanism for your API endpoint.

► Additional settings

Lambda will add the necessary permissions for Amazon API Gateway to invoke your Lambda function from this trigger.
[Learn more](#) about the Lambda permissions model.

Cancel Add

Security then click on open

Add an API to your Lambda function to create an HTTP endpoint that invokes your function. API Gateway supports two types of RESTful APIs: HTTP APIs and REST APIs. [Learn more](#)

API
Create a new API or attach an existing one.

Create an API

API type

HTTP API
Create an HTTP API.

REST API
Create a REST API.

Security
Configure the security mechanism for your API endpoint.

Open

IAM

Open

API key

Lambda will add the necessary permissions for Amazon API Gateway to invoke your Lambda function from this trigger.
[Learn more](#) about the Lambda permissions model.

Cancel Add

Then go to additional setting

Add an API to your Lambda function to create an HTTP endpoint that invokes your function. API Gateway supports two types of RESTful APIs: HTTP APIs and REST APIs. [Learn more](#)

API
Create a new API or attach an existing one.

Create an API

API type

HTTP API
Create an HTTP API.

REST API
Create a REST API.

Security
Configure the security mechanism for your API endpoint.

Open

IAM

Open

API key

Lambda will add the necessary permissions for Amazon API Gateway to invoke your Lambda function from this trigger.
[Learn more](#) about the Lambda permissions model.

Cancel Add

Deployment stage: myDeployment

API name
Choose a name for your API. API names don't need to be unique.

Deployment stage
The name of your API's deployment stage.

Cross-origin resource sharing (CORS)
CORS is required to call your API from a webpage that isn't hosted on the same domain. To enable CORS for a REST API, set the Access-Control-Allow-Origin header in the response object that you return from your function code.

Enable metrics and error logging
Record latency and error metrics in Amazon CloudWatch, and log errors in Amazon CloudWatch Logs. Standard CloudWatch and CloudWatch Logs pricing applies.

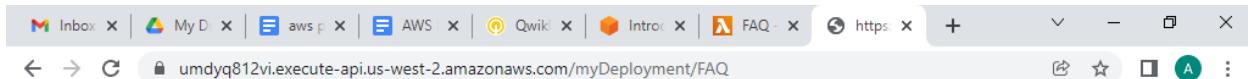
Binary media types
Specify response types that API Gateway should treat as binary data instead of text. To treat all responses as binary data, use */*. If you enter one or more specific types, you must also set the Content-Type header in the response object that you return from your function code.

first you scroll down and Then click on add

Task 2: Test the Lambda function

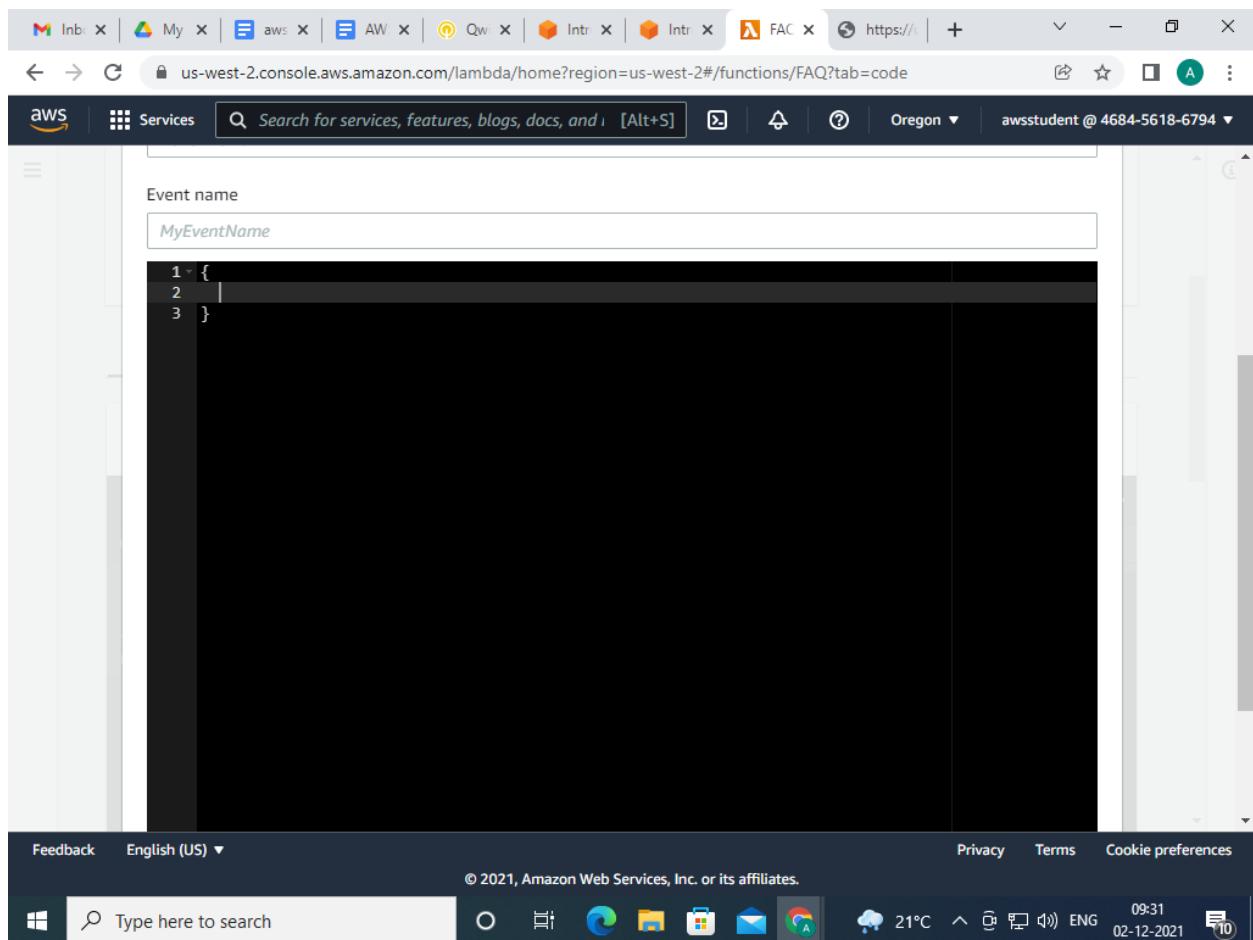
The screenshot shows the AWS Lambda configuration page for a function named 'FAQ'. The 'Configuration' tab is selected. On the left, a sidebar lists options like General configuration, Triggers (which is selected and highlighted in orange), Permissions, Destinations, Environment variables, Tags, VPC, Monitoring and operations tools, and Concurrency. The main area displays a 'Triggers (1)' section with a table. The table has one row for an 'API Gateway' trigger, which is highlighted with a blue border. A context menu is open over this row, showing options: Open link in new tab, Open link in new window, Open link in incognito window, Save link as..., Copy link address (which is highlighted in gray), and Inspect. At the bottom of the browser window, the status bar shows the URL 'https://umdyq812vi.execute-api.us-west-2.amazonaws.com/n' and the text 'Amazon Web Services, Inc. or its affiliates.'

Copy link paste in another tab.



Then close FAQ browser then it show lambda management console

Go to test



Then click on create

The screenshot shows the AWS Lambda console interface. At the top, a green banner indicates that the test event 'BasicTest' was successfully saved. Below this, the 'Code' tab is selected in the navigation bar. The main area displays the 'Code source' tab of the 'index.js' file. The code editor shows the following JavaScript function:

```
56     "q": "How do I compile my AWS Lambda function Java code?",  
57     "a": "You can use standard tools like Maven or Gradle to compile your Lambda fu  
58 }, {  
59     "q": "What is the JVM environment Lambda uses for execution of my function?",  
60     "a": "Lambda provides the Amazon Linux build of openjdk 1.8."  
61 }  
62 }  
63 }  
64  
65 exports.handler = function(event, context) {  
66     var rand = Math.floor(Math.random() * json.questions.length);  
67     console.log("Question selected: " + rand);  
68     return {  
69         statusCode: 200,  
70         body: JSON.stringify(json.questions[rand])  
71     };  
72 }  
73 }
```

The browser's address bar shows the URL: `https://us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2#/functions/FAQ?tab=code`. The bottom of the screen shows the Windows taskbar with various pinned icons.

Click on monitor tab

The screenshot shows the AWS Lambda Monitoring page. At the top, there is a success message: "The test event BasicTest was successfully saved." Below this, there are tabs for Metrics, Logs, and Traces, with Metrics selected. There are also links to View logs in CloudWatch, View X-Ray traces in ServiceLens, View Lambda Insights, and View profiles in CodeGuru.

CloudWatch metrics Info

Lambda sends runtime metrics for your functions to Amazon CloudWatch. The metrics shown are an **aggregate** view of all function runtime activity. To view metrics for the unqualified or \$LATEST resource, choose an option in the dropdown list. To view metrics for a specific function version or alias, choose the qualifier name on the Function details page, and select the Monitoring page.

Filter by **Function** ▾

Time range: 1h 3h 12h 1d 3d 1w Custom Add to dashboard

Three line charts are displayed:

- Invocations**: Shows a single data point at 1 invocation.
- Duration**: Shows a single data point at approximately 0.5 seconds.
- Error count and success rate**: Shows a single data point at 1 error and a success rate of 100%.

Feedback English (US) ▾ © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences https://us-west-2.console.aws.amazon.com/lambda/home?r... 09:35 02-12-2021

The test event **BasicTest** was successfully saved.

Metrics Logs Traces

[View logs in CloudWatch](#) [View X-Ray traces in ServiceLens](#) [View Lambda Insights](#)

[View profiles in CodeGuru](#)

CloudWatch metrics [Info](#)

Lambda sends runtime metrics for your functions to Amazon CloudWatch. The metrics shown are an **aggregate** view of all function runtime activity. To view metrics for the unqualified or \$LATEST resource, choose an option in the dropdown list. To view metrics for a specific function version or alias, choose the qualifier name on the Function details page, and select the Monitoring page.

Filter by **Function**

1h 3h 12h 1d 3d 1w Custom [C](#) Add to dashboard

Invocations	Duration	Error count and success rate
Count 2 1	Milliseconds 51.9 51.3 50.6	Count No unit 1 0.5 99.5

Feedback English (US) ▾ Privacy Terms Cookie preferences

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

Type here to search

View logs in cloud watch

Click on Log Stream

The screenshot shows the AWS CloudWatch Log Groups interface. The left sidebar is titled "CloudWatch" and includes sections for Favorites, Dashboards, Alarms, Logs (with Log groups selected), Metrics, Events, Application monitoring, Insights, Settings, and Getting Started. The main content area shows the path "CloudWatch > Log groups > /aws/lambda/FAQ". Below this, there are buttons for "Actions", "View in Logs Insights", and "Search log group". A section titled "Log group details" is expanded. At the top of the log streams list are buttons for "Log streams" (selected), Metric filters, Subscription filters, Contributor Insights, and Tags. The "Log streams" section displays one entry:

Log stream	Last event time
2021/12/02/[\$LATEST]fdddc16e...	2021-12-02 09:23:13 (UTC+05:30)

At the bottom of the page are links for Feedback, English (US) (dropdown), Privacy, Terms, and Cookie preferences. The taskbar at the bottom includes icons for File, Home, Task View, Start, Taskbar settings, Edge browser, File Explorer, Google Photos, Mail, and Google Chrome. It also shows the date (02-12-2021), time (09:38), battery level (10%), and a weather icon indicating 21°C.

The screenshot shows the AWS Lambda console interface. A new API Gateway trigger is being configured. The 'Deployment stage' field is set to 'myDeployment'. Under 'Cross-origin resource sharing (CORS)', there is a checkbox for 'Enable metrics and error logging' which is unchecked. Below it, a note states: 'Record latency and error metrics in Amazon CloudWatch, and log errors in Amazon CloudWatch Logs. Standard CloudWatch and CloudWatch Logs pricing applies.' In the 'Binary media types' section, 'image/png' is listed in a text input field, with a 'Remove' button next to it and an 'Add' button below. A note below this section says: 'Lambda will add the necessary permissions for Amazon API Gateway to invoke your Lambda function from this trigger. [Learn more](#) about the Lambda permissions model.' At the bottom of the configuration panel, there are links for 'Feedback', 'English (US) ▾', 'Privacy', 'Terms', and 'Cookie preferences'. The status bar at the bottom of the browser window shows the date and time as '02-12-2021 09:18'.

Practical No. 5

Introduction to Amazon DynamoDB

Aim: A) Create a new table

- B) Add data**
- C) Modify existing items**
- D) Query the table**
- E) Delete the table**

Introduction to Amazon DynamoDB

Task 1: Create a new Table

In this task, you will create a new table in DynamoDB named music. Each table requires a primary key that is used to partition data across DynamoDB servers. A table can also have a sort key uniquely identifying each item in a DynamoDB table.

The screenshot shows the AWS website with a search bar at the top containing the query "Dyn". Below the search bar, there's a navigation menu with links to Contact Us, Support, English, My Account, Sign In, and a "Complete Sign Up" button. The main content area is titled "PRODUCTS" and features a section for "Amazon DynamoDB" which is described as a "Managed NoSQL database". It includes links for Pricing, Documentation, and Calculator. Below this, there are sections for RELATED PAGES (Amazon DynamoDB Partners), TUTORIALS (Create and Query a NoSQL Table with DynamoDB, Create and manage DynamoDB tables), and BLOGS (Blog posts about Amazon DynamoDB). A sidebar on the right is titled "Blogs" and "Read the latest from the AWS Chief Evangelist and team". At the bottom of the page, there are several navigation links: Amazon EMR Serverless, Amazon Managed Streaming for Apache Kafka (Amazon), and Amazon Redshift Serverless (Preview). The browser status bar at the bottom shows the URL https://aws.amazon.com/dynamodb/?nc2-type_a.

The screenshot shows the AWS Management Console search results for "Dyn". The search bar at the top contains the query "Dyn". The results list various AWS services and tools, including CloudFormation, Inspector, CloudTrail, Amazon Macie, AWS Single Sign-On, Certificate Manager, Key Management Service, CloudHSM, Directory Service, WAF & Shield, AWS Firewall Manager, Artifact, Security Hub, Detective, AWS Audit Manager, AWS Signer, AWS Network Firewall, AWS Cost Management, AWS Cost Explorer, AWS Budgets, AWS Marketplace Subscriptions, AWS Application Cost Profiler, Kinesis Video Streams, AWS Amplify, AWS AppSync, Device Farm, and Amazon Location Service. To the right of the search results, there are promotional sections for "Free AWS Training" (a six-hour course), "AWS Certification" (forwarding career), "AWS Training" (digital courses for skills), and "Have feedback?" (submit feedback for the AWS Management Console). The browser status bar at the bottom shows the URL <https://us-west-2.console.aws.amazon.com/dynamodb/home?region=us-west-2>.

The screenshot shows the new Amazon DynamoDB console homepage. The top navigation bar includes tabs for 'Students study material sh...', 'Students Study Material - C...', 'Sem III / Amazon Web Serv...', 'aws practical index with qv...', 'Introduction to Amazon D...', 'Service | Amazon Dynam...', and a '+' icon. The search bar says 'Search for services, features, blogs, docs, and more' with the keyboard shortcut '[Alt+S]'. The user information 'Oregon' and 'awsstudent @ 0672-6151-0747' is at the top right.

The main content area has a blue header: 'The new DynamoDB console is now complete, and becomes your default experience'. It states: 'Following the preview phase in which we analyzed and incorporated your feedback, we have completed the new DynamoDB console, making it even easier for you to manage your data and resources. Let us know what you think. You can still choose to return to the previous console from the navigation pane.'

The central part of the page features the heading 'Amazon DynamoDB' and the subtext 'A fast and flexible NoSQL database service for any scale'. Below this, a paragraph explains: 'DynamoDB is a fully managed, key-value, and document database that delivers single-digit-millisecond performance at any scale.'

On the right side, there are two sections: 'Get started' (with a 'Create table' button) and 'Pricing' (with a link to learn more about pricing). At the bottom left, there's a 'How it works' section with a 'What is Amazon DynamoDB?' video thumbnail and a 'Copy link' button.

The footer contains links for 'Feedback', 'English (US)', 'Privacy', 'Terms', and 'Cookie preferences'. The system status bar at the bottom shows 'EN', '26°C Sunny', '10:35', and the date '05-12-2021'.

This screenshot shows the 'Tables' page within the DynamoDB service. The top navigation bar is identical to the previous screenshot. The left sidebar shows the 'Tables' section is selected. The main content area displays a table titled 'Tables (0) Info'. The table has columns: Name (sorted), Status, Partition key, Sort key, Indexes, Read capacity mode, Write capacity mode, Table class, and Encryption. A message at the bottom says 'You have no tables in this account in this AWS Region.' A 'Create table' button is located at the bottom of the table area.

The footer and system status bar are also present at the bottom of the screen.

The new DynamoDB console is now complete, and becomes your default experience

Following the preview phase in which we analyzed and incorporated your feedback, we have completed the new DynamoDB console, making it even easier for you to manage your data and resources. Let us know what you think. You can still choose to return to the previous console from the navigation pane.

DynamoDB

- Dashboard
- Tables**
 - Items **New**
 - PartQL editor **New**
 - Backups
 - Exports to S3
 - Reserved capacity
- ▼ DAX
 - Clusters
 - Subnet groups
 - Parameter groups
 - Events
- Tell us what you think
- Return to the previous console experience

Tables (0) Info

Music Any table tag

Name Status Partition key Sort key Indexes Read capacity mode Write capacity mode Table class Encryption

You have no tables in this account in this AWS Region.

Create table

<https://us-west-2.console.aws.amazon.com/dynamodbv2/home?region=us-west-2#create-table>

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.

Between 3 and 255 characters, containing only letters, numbers, underscores (_), hyphens (-), and periods (.)

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.
 String
1 to 255 characters and case sensitive.

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.
 String
1 to 255 characters and case sensitive.

Settings

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.

Feedback English (US) Type here to search © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences EN 26°C Sunny 1039 05-12-2021

The screenshot shows the AWS DynamoDB console interface. A modal window is open for creating a new table. The table name is 'Music'. In the 'Table class' section, it's selected 'Using DynamoDB Standard table class'. Under 'Tags', there are no tags associated with the resource. A note at the bottom of the modal states: 'This table will be created with auto scaling disabled. You do not have permissions to enable auto scaling.' At the bottom right of the modal are 'Cancel' and 'Create table' buttons.

Task 2: ADD DATA

The screenshot shows the AWS DynamoDB console interface. On the left, the navigation pane is visible with sections like 'Dashboard', 'Tables', 'DAX', and 'Tell us what you think'. The 'Tables' section is currently active, showing a list of tables. One table, 'Music', is listed with the following details: Name: Music, Status: Active, Partition key: Artist (String), Sort key: Song (String), Read capacity mode: Provisioned (5), Write capacity mode: Provisioned (5), and Table class: DynamoDB Standard. A message at the top of the page says: 'The new DynamoDB console is now complete, and becomes your default experience. Following the preview phase in which we analyzed and incorporated your feedback, we have completed the new DynamoDB console, making it even easier for you to manage your data and resources. Let us know what you think. You can still choose to return to the previous console from the navigation pane.' Another message below it says: 'Your Music table was created with auto scaling turned off. Try enabling auto scaling from table settings.'

The screenshot shows the AWS DynamoDB console. A modal at the top left says: "The new DynamoDB console is now complete, and becomes your default experience. Following the preview phase in which we analyzed and incorporated your feedback, we have completed the new DynamoDB console, making it even easier for you to manage your data and resources. Let us know what you think. You can still choose to return to the previous console from the navigation pane." Below this, another modal says: "Your Music table was created with auto scaling turned off. Try enabling auto scaling from table settings." On the left sidebar, under the "Tables" section, there is a link to "Items New". The main content area shows a table titled "Tables (1) Info" with one row for "Music". The table columns are: Name (sorted), Status, Partition key, Sort key, Indexes, Read capacity mode, Write capacity mode, and Table class. The "Music" row has "Active" status, "Artist (String)" as the partition key, "Song (String)" as the sort key, 0 indexes, Provisioned (5) for both read and write capacity modes, and "DynamoDB Standard" as the table class.

The screenshot shows the AWS DynamoDB console. A modal at the top left says: "The new DynamoDB console is now complete, and becomes your default experience. Following the preview phase in which we analyzed and incorporated your feedback, we have completed the new DynamoDB console, making it even easier for you to manage your data and resources. Let us know what you think. You can still choose to return to the previous console from the navigation pane." Below this, another modal says: "On this page, query and scan for items. Choose a table to get started. Standard query and scanning prices applies." On the left sidebar, under the "Items" section, there is a link to "PartiQL editor New". The main content area shows a table titled "Tables (1) Info" with one row for "Music". The table columns are: Name (sorted), Status, Partition key, Sort key, Indexes, Read capacity mode, Write capacity mode, and Table class. The "Music" row has "Active" status, "Artist (String)" as the partition key, "Song (String)" as the sort key, 0 indexes, Provisioned (5) for both read and write capacity modes, and "DynamoDB Standard" as the table class. There is also an "Autopreview" button in the top right of the main content area.

The new DynamoDB console is now complete, and becomes your default experience

Following the preview phase in which we analyzed and incorporated your feedback, we have completed the new DynamoDB console, making it even easier for you to manage your data and resources. Let us know what you think. You can still choose to return to the previous console from the navigation pane.

DynamoDB

- Dashboard
- Tables
- Items New**
- PartiQL editor New
- Backups
- Exports to S3
- Reserved capacity

▼ DAX

- Clusters
- Subnet groups
- Parameter groups
- Events

Tell us what you think

Return to the previous console experience

Items Info

Tables (1) C X

Tag: Any table tag

Find tables by name

Music

Items returned (0)

Actions Create item

The query did not return any results.

https://us-west-2.console.aws.amazon.com/dynamodbv2/home?region=us-west-2#edit-item?table=Music&ref=%23item-explorer%3Ftable%3DMusic&route=ROUTE_ITEM_EXPLORER&itemMode=1

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

EN 26°C Sunny 1042 05-12-2021

Students study material sha... **Students Study Material...** **Sem III / Amazon Web Serv...** **aws practical index with q...** **Introduction to Amazon D...** **Edit Item | Amazon Dyn...**

Feedback English (US) ▾

Type here to search

Cancel Create item

© 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

EN 26°C Sunny 1043 05-12-2021

The screenshot shows three sequential views of the AWS DynamoDB console.

Step 1: Create item

The first window shows the "Create item" dialog for a "Music" table. The "Artist" attribute is set to "Pink Floyd". The "Song" attribute is set to "Money". The "Album" attribute is set to "The Dark Side of the Moon". The "Year" attribute is set to "1973".

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

Step 2: Item saved successfully

The second window shows the "Items" page for the "Music" table. A green success message states: "The item has been saved successfully." The table data shows one item: "Artist": "Pink Floyd", "Song": "Money", "Album": "The Dark Si...", "Year": "1973".

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

Step 3: Item details

The third window shows the detailed view for the item "Pink Floyd" in the "Music" table. The item details are: "Artist": "Pink Floyd", "Song": "Money", "Album": "The Dark Side of the Moon", "Year": "1973".

Screenshot of the AWS DynamoDB console showing the creation of a new item in the 'students' table.

The 'Create item' dialog shows the following attributes:

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

After saving, a success message is displayed: "The item has been saved successfully."

The 'Items' page lists the 'students' table with one item:

	Artist	Song	Album	LengthS...	Year
<input type="checkbox"/>	Psy	Gangnam S...	Psy 6 (Six R...	219	2011

The screenshot shows the AWS DynamoDB Item editor interface. On the left, there's a navigation sidebar with links like Dashboard, Tables, Items (New), PartiQL editor, Backups, Exports to S3, Reserved capacity, DAX, Clusters, Subnet groups, Parameter groups, and Events. Below the sidebar, there are two buttons: 'Tell us what you think' and 'Return to the previous console experience'. The main area is titled 'Item editor' and has a sub-section 'Attributes'. It lists five attributes with their values: Artist (Psy), Song (Gangnam Style), Album (Psy 6 (Six Rules), Part 1), LengthSeconds (219), and Year (2011). There are buttons for 'Add new attribute' and 'Save changes'.

This screenshot is identical to the one above it, showing the AWS DynamoDB Item editor interface. The table attributes and their values remain the same: Artist (Psy), Song (Gangnam Style), Album (Psy 6 (Six Rules), Part 1), LengthSeconds (219), and Year (2012). The 'Save changes' button is visible at the bottom right.

This screenshot is identical to the ones above it, showing the AWS DynamoDB Item editor interface. The table attributes and their values remain the same: Artist (Psy), Song (Gangnam Style), Album (Psy 6 (Six Rules), Part 1), LengthSeconds (219), and Year (2011). The 'Save changes' button is visible at the bottom right.

Screenshot of the AWS DynamoDB Item Editor interface showing the creation of a new item in the 'students' table.

Attributes

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

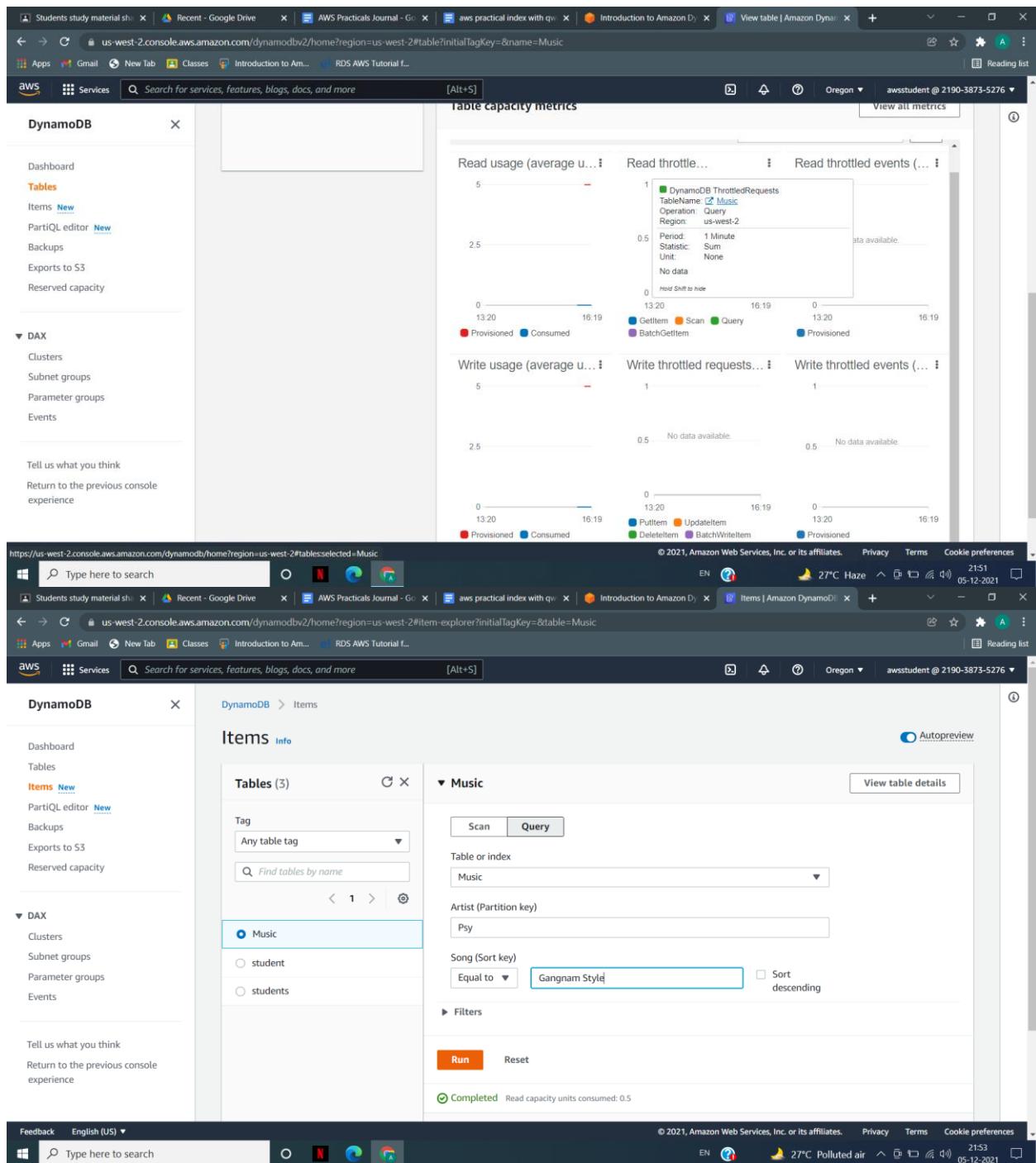
Items

Tables (3)

- Music
- student
- students

Items returned (1)

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



The image displays three vertically stacked screenshots of the AWS DynamoDB Items page, illustrating how to filter data using the Query feature.

Screenshot 1: Shows a basic query setup. The "Table or index" dropdown is set to "Music". The "Filters" section shows an attribute named "student" with a type of "String" and a condition of "Equal to". The value field contains "student".

Screenshot 2: Shows a more complex query. The "Table or index" dropdown is set to "Music". The "Filters" section shows an attribute named "Year" with a type of "Number" and a condition of "Equal to". The value field contains "1971".

Screenshot 3: Shows the results of the query. The "Items returned (0)" section indicates no results were found. The status message "Completed" and "Read capacity units consumed: 0.5" are also visible.

Screenshot of the AWS DynamoDB console showing three tables: Music, student, and students.

Name	Status	Partition key	Sort key	Indexes	Read capacity mode	Write capacity mode	Table class
Music	Active	Artist (String)	Song (String)	0	Provisioned (5)	Provisioned (5)	DynamoDB Standard
student	Active	D1 (String)	D2 (String)	0	Provisioned (5)	Provisioned (5)	DynamoDB Standard
students	Active	Artist (String)	Song (String)	0	Provisioned (5)	Provisioned (5)	DynamoDB Standard

Delete table

You are about to delete a table.

- Music

Delete all CloudWatch alarms for this table.

Create a backup of this table before deleting it.
If you do not select this check box, you will not be able to restore data being deleted.

To confirm the deletion of this table, type **delete** in the box.

delete

Cancel Delete table

The screenshots show the AWS DynamoDB console interface across three different browser sessions. In each session, the user is deleting the 'Music' table.

Screenshot 1: The user is in the 'Delete table' confirmation dialog. The table 'Music' is selected. A checkbox for 'Delete all CloudWatch alarms for this table.' is checked. A note below states: 'If you do not select this check box, you will not be able to restore data being deleted.' A text input field contains the word 'delete'. The 'Delete table' button is highlighted in orange.

Screenshot 2: The user has confirmed the deletion. The 'Delete table' dialog now shows a red 'X' next to 'Music'. The 'Go to tables' button is visible at the bottom right.

Screenshot 3: The user has completed the deletion process. The 'Delete table' dialog is closed, and the main DynamoDB table list shows the 'Music' table has been successfully deleted.

The screenshot shows the AWS DynamoDB Items page. The left sidebar includes links for Dashboard, Tables (with 'Items' selected), PartiQL editor, Backups, Exports to S3, Reserved capacity, Clusters, Subnet groups, Parameter groups, and Events. A feedback section at the bottom asks for user input and provides a link to return to the previous console experience.

The main content area displays a search interface for tables. A search bar at the top contains the query 'music'. Below it, a table titled 'Tables (2)' shows two entries: 'Tag' and 'No matches'. A message states, 'We cannot find a match.' A 'Clear filter' button is present. On the right, a note says, 'On this page, query and scan for items. Choose a table to get started. Standard query and scanning prices applies.'

The browser's address bar shows the URL: us-west-2.console.aws.amazon.com/dynamodbv2/home?region=us-west-2#item-explorer?initialTagKey=. The status bar at the bottom indicates the date as 05-12-2021 and the time as 21:56.

Practical No. 6

Introduction to Amazon Redshift

- Aim:**
- 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**

Introduction to Virtual Private Cloud (VPC)

Lab Steps

Logging in to the Amazon Web Services Console

Creating a VPC

Creating a VPC subnet

Creating a VPC Internet Gateway

Connecting the Internet Gateway to the VPC Route Table

Creating an EC2 instance

Allocating and Associating an Elastic IP

- A) Launch an amazon redshift cluster**

AccessDeniedException
User: arn:aws:sts::771545426752:federated-user/awsstudent is not authorized to perform: redshift-serverless:DescribeConfiguration because no identity-based policy allows the redshift-serverless:DescribeConfiguration action

Analytics

Amazon Redshift

Accelerate your time to value with fast, easy, and secure analytics at scale.

Amazon Redshift makes it easier for you to run and scale analytics without having to manage their data warehouse. Get insights running real-time and predictive analytics on all your data across your operational databases, data lake, data warehouse, and thousands of third-party datasets.

Get to powerful insights fast

The Amazon Redshift serverless experience makes it easy for customers to run and scale analytics without having to provision and manage their data warehouse. Simply load and query data.

Try Amazon Redshift Serverless (Preview)

How it works

English (US) ▾ © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 11:24 AM

Cluster configuration

Cluster identifier
This is the unique key that identifies a cluster.

The identifier must be from 1-63 characters. Valid characters are a-z (lowercase only) and - (hyphen).

What are you planning to use this cluster for?

Production
Configure for fast and consistent performance at the best price.

Free trial
Configure for learning about Amazon Redshift. This configuration is free for a limited time if your organization has never created an Amazon Redshift cluster.

Choose the size of the cluster

I'll choose **Help me choose**

Node type [Info](#)
Choose a node type that meets your CPU, RAM, storage capacity, and drive type requirements.

Range (1-32)

Number of nodes
Enter the number of nodes that you need.

Range (1-32)

Database configurations

Admin user name

Enter a login ID for the admin user of your DB instance.

The name must be 1-128 alphanumeric characters, and it can't be a [reserved word](#).

[Auto generate password](#)

Amazon Redshift can generate a password for you, or you can specify your own password.

Admin user password

[Show password](#)

Must be 8-64 characters long. Must contain at least one uppercase letter, one lowercase letter and one number. Can be any printable ASCII character except "/", "", or "@".

Associated IAM roles (1) [Info](#)

[Set default](#)[Manage IAM roles](#)

<input type="text"/> Search for associated IAM role by name, status, or role type		
<input type="checkbox"/>	IAM roles	Status
<input type="checkbox"/>	Redshift-Role	Not applied

Additional configurations [Use defaults](#)

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

▼ Network and security

Virtual private cloud (VPC)

This VPC defines the virtual networking environment for this cluster.

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

VPC security groups

This VPC security group defines which subnets and IP ranges the cluster can use in the VPC.

[Cluster subnet group](#)

▼ Database configurations

Database name

Specify a database name to create an additional database.

The name must be 1-64 alphanumeric characters (lowercase only), and it can't be a **reserved word**.

Database port

Port number where the database accepts inbound connections. You can't change the port after the cluster has been created.

The port must be numeric (1150-65535).

Parameter groups

Defines database parameter and query queues for all the databases.

Default parameter group for redshift-1.0



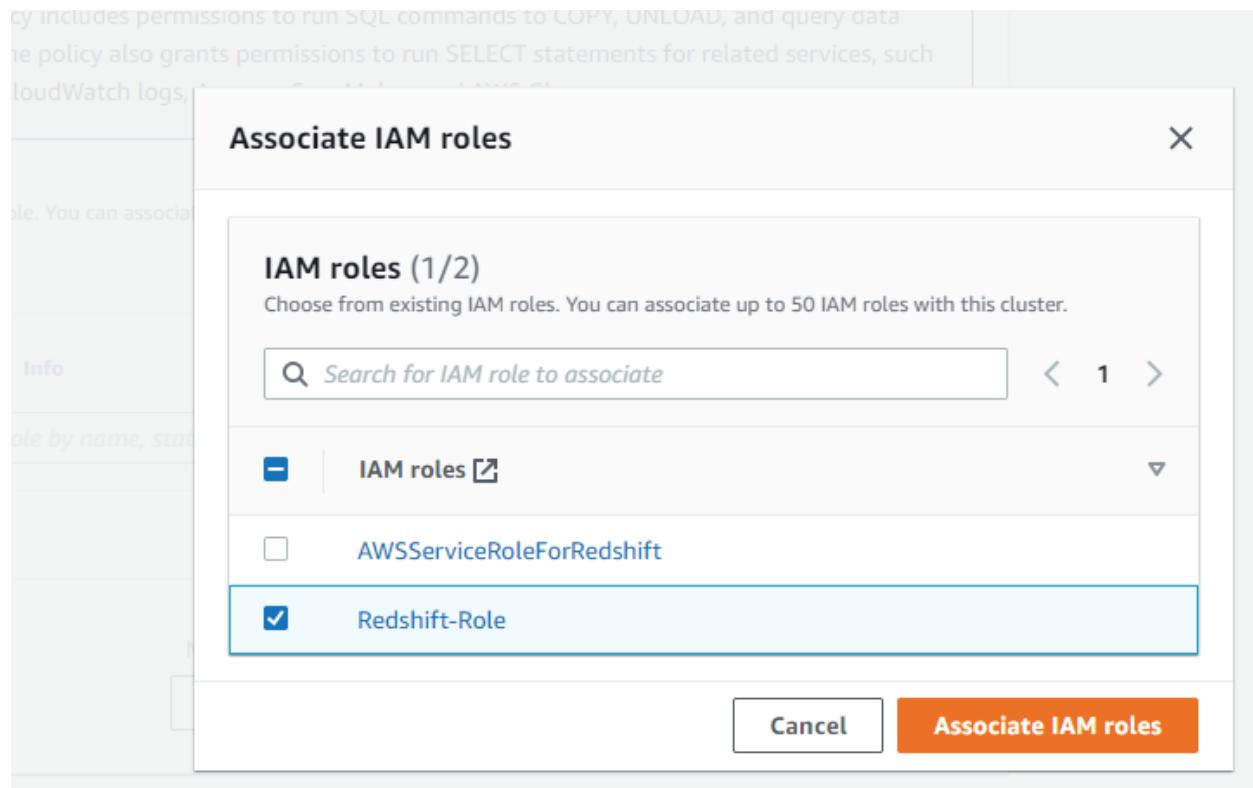
Encryption

Encrypt all data on your cluster.

Disabled

Use AWS Key Management Service (AWS KMS)

Use a hardware security module (HSM)



The screenshot shows the "Clusters" page in the Amazon Redshift console. It includes sections for connecting to Redshift clusters, such as "Query data using Redshift query editor" (with a "Query data" button), "Work with your client tools" (with a "Cluster" dropdown and copy buttons for JDBC and ODBC URLs), and "Choose your JDBC or ODBC driver" (with a "Driver" dropdown set to "JDBC 4.2 without AWS SDK (.jar)"). Below this is a "Clusters (0) Info" section with a search bar and a table header for managing clusters. The table shows columns for Cluster, Cluster namespace, Status, Storage capacity us..., CPU utilization, Snapshots, Notifications, and Actions. A message at the bottom states "No clusters".

The screenshot shows the 'Clusters' page in the Amazon Redshift console. There is one cluster listed:

Cluster	Cluster namespace	Status
lab	2053c860-a0c5-40db-...	Modifying Creating

This section provides connectivity options for Amazon Redshift:

- Query data using Redshift query editor:** Use the query editor v2 to run queries in your Redshift cluster. A 'Query data' button is available.
- Work with your client tools:** You can connect to Amazon Redshift from your client tools, such as SQL clients, business intelligence (BI) tools, and extract, transform, load (ETL) tools, using JDBC or ODBC drivers. It includes a 'Cluster' dropdown for selecting the identifier, and buttons to 'Copy JDBC URL' and 'Copy ODBC URL'.
- Choose your JDBC or ODBC driver:** Use JDBC or ODBC drivers to connect to Amazon Redshift from your client tools, such as SQL clients, BI tools, and ETL tools. We recommend using the new Amazon Redshift-specific drivers for better performance and scalability. It includes a 'Driver' dropdown set to 'JDBC 4.2 without AWS SDK (.jar)' and a 'Download driver' button.

The screenshot shows the 'Clusters' page again, but the cluster 'lab' is now in the 'Available' state:

Cluster	Cluster namespace	Status	CPU utilization
lab	2053c860-a0c5-40db-...	Available	44%

B Launch Pgweb to communicate with the redshift cluster

The screenshot shows the Amazon Redshift Query Editor v2 interface. At the top, there is a blue banner with the message: "Amazon Redshift query editor v2 is now available. Query editor v2 provides new features such as multistatement query execution, query parameterization, query versioning, visualizations, and query sharing. Learn more" and a "Go to query editor v2" button. Below the banner, the navigation bar includes "Amazon Redshift > Query editor" and tabs for "Editor", "Query history", "Saved queries", and "Scheduled queries". A sidebar on the left lists various services: PROVISIONED..., CLUSTERS, QUERIES, EDITOR (which is selected and highlighted in orange), DATABASES, CONFIG, MARKETPLACE, ADVISOR, ALARMS, and EVENTS. The main content area shows a "Resources" panel with dropdown menus for "Select database" and "Select schema", and a search bar for "Filter tables". A large text input field labeled "Query 1" is present, with the number "1" inside it. To the right of the input field are several icons for query execution and monitoring.

Connect to database

Connection
Select a recent database connection or create a new database connection.

Use a recent connection
 Create a new connection

Authentication

Temporary credentials
Use the GetClusterCredentials IAM permission and your database user to generate temporary access credentials. [Learn more](#)

AWS Secrets Manager
Use a stored secret to authenticate access. [Learn more](#)

Cluster
lab (Available)

Database name
labdb

Database user
User name authorized to access your database.
master

Cancel **Connect**

The screenshot shows the Amazon Redshift Query Editor interface. At the top, a blue banner informs about 'Amazon Redshift query editor v2 is now available' and provides a link to 'Go to query editor v2'. Below the banner, the navigation bar includes 'Amazon Redshift > Query editor' and tabs for 'Editor' (which is selected), 'Query history', 'Saved queries', and 'Scheduled queries'. On the left, a sidebar titled 'Resources' shows 'No resources' under 'labdb' database and 'public' schema. The main area displays a query editor window with 'Status' set to 'Connected' (indicated by a green circle with a checkmark). The query tab is labeled 'Query 1'. The query itself is a single line: '1 CREATE TABLE users ('. The editor also features standard SQL navigation keys like backspace, forward slash, and asterisk. At the bottom, there are buttons for 'Run', 'Save', 'Schedule', and 'Clear', along with a 'Send feedback' link.

Task 3 Create a table

This screenshot is similar to the one above but includes a vertical sidebar on the left containing icons for 'PROVISIONED...', 'CLUSTERS', 'QUERIES', 'EDITOR' (which is highlighted in orange), 'DATABASES', 'CONFIG', 'MARKETPLACE', 'ADVISOR', 'ALARMS', and 'EVENTS'. The main interface is identical to the first screenshot, showing the 'Editor' tab selected. The 'Resources' sidebar still shows 'No resources'. The 'Query 1' editor contains the full SQL code for creating a 'users' table:

```
1 CREATE TABLE users (
2     userid INTEGER NOT NULL,
3     username CHAR(8),
4     firstname VARCHAR(30),
5     lastname VARCHAR(30),
6     city VARCHAR(30),
7     state CHAR(2),
8     email VARCHAR(100),
9     phone CHAR(14),
10    likesports BOOLEAN,
11    liketheatre BOOLEAN,
12    likeconcerts BOOLEAN,
13    likejazz BOOLEAN,
14    likeclassical BOOLEAN,
15    likeopera BOOLEAN,
```

The 'Run' button at the bottom of the editor is highlighted in orange, indicating it has been clicked.

Status  Connected | data

 **Query 1** | +

```
8   email VARCHAR(100),
9   phone CHAR(14),
10  likesports BOOLEAN,
11  liketheatre BOOLEAN,
12  likeconcerts BOOLEAN,
13  likejazz BOOLEAN,
14  likeclassical BOOLEAN,
15  likeopera BOOLEAN,
16  likerock BOOLEAN,
17  likevegas BOOLEAN,
18  likebroadway BOOLEAN,
19  likemusicals BOOLEAN
20 );
```

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

4. Load sample data from amazon S3

Query 1 | + | ▾

```
1 COPY users FROM 's3://awssampledbuswest2/ticket/allusers_pipe.txt'
2 CREDENTIALS 'aws_iam_role=arn:aws:iam::771545426752:role/Redshift-Role'
3 DELIMITER '|';
```

Run Save Schedule Clear Send feedback

Query results Table details

Query 209

Completed, started on December 04, 2021 at 12:01:58
ELAPSED TIME: 00 m 08 s

Execution Data Visualize

E Query data

```
1 > 10
11 SELECT userid, firstname, lastname, city, state
12 FROM users
13 WHERE likesports AND NOT likeopera AND state = 'OH'
14 ORDER BY firstname;
```

Run **Save** **Schedule** **Clear** **Send feedback**

Query results **Table details**

Query 265 **Execution** **Data** **Visualize**

Completed, started on December 04, 2021 at 12:06:23
ELAPSED TIME: 00 m 08 s

Rows returned (18) **Export**

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

```
10
11 SELECT
12   city,
13   COUNT(*) AS count
14 FROM users
15 WHERE likejazz
16 GROUP BY city
17 ORDER BY count DESC
18 LIMIT 10;
```

Run Save Schedule Clear Send feedback

Query results Table details

Query 277

Completed, started on December 04, 2021 at 12:07:49
ELAPSED TIME: 00 m 02 s

Rows returned (10)

Search rows Export ▾

city	count
Dover	33
Charleston	30
Hartford	28

© 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

28°C Sunny 12:07 PM 12/4/2021

Practical No. 7

Introduction to AWS Key management Service

- Aim:
- 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

Create Your First Amazon RDS Database

Lab Steps

Logging in to the Amazon Web Services Console

Creating an RDS Subnet Group

Setting up Security Group Rules for Connecting to the RDS Instance

Creating a Database Using RDS

Starting an AWS Systems Manager Session Manager Browser Shell Session

Connecting to RDS and Creating a Database Table

Deleting an RDS Database

← Introduction to AWS Key Management Service



End Lab 00:48:29

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](#)

Introduction to AWS Key Management Service



SPL-87 - Version 2.0.18

© 2021 Amazon Web Services, Inc. and 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

1. Create your KMS Master Key

Lab Overview
Topics covered
Prerequisites
Start Lab
Task 1: Create Yc
Task 2: Configur
In An S3 Bucket
Task 3: Upload a
And Encrypt It
Task 4: Access T
Task 5: Monitor I
CloudTrail Logs
Task 6: Manage I
End Lab
Conclusion
Additional Reso

All services

Compute	Quantum Technologies	Security, Identity, & Compliance
EC2	Amazon Braket	IAM
Lightsail		Resource Access Manager
Lambda		Cognito
Batch		Secrets Manager
Elastic Beanstalk		GuardDuty
Serverless Application Repository		Inspector
AWS Outposts		Amazon Macie
EC2 Image Builder		AWS Single Sign-On
AWS App Runner		Certificate Manager
Containers		Key Management Service

Key Management Service (KMS)

AWS managed keys
Customer managed keys
Custom key stores

Security, Identity & Compliance

AWS Key Management Service

Easily create keys and control encryption across AWS and beyond

AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and manage keys and control the use of encryption across a wide range of AWS services. KMS is a secure and resilient service that uses FIPS 140-2 validated hardware security modules to isolate and protect your keys.

Get started now

You can create a key by clicking the button below.

Create a key



aWS Services Search for services, features, blogs, docs, and more [Alt+S]

Key Management Service (KMS)

AWS managed keys
Customer managed keys
Custom key stores

KMS > Customer managed keys > Create key

Configure key

Step 1 of 5

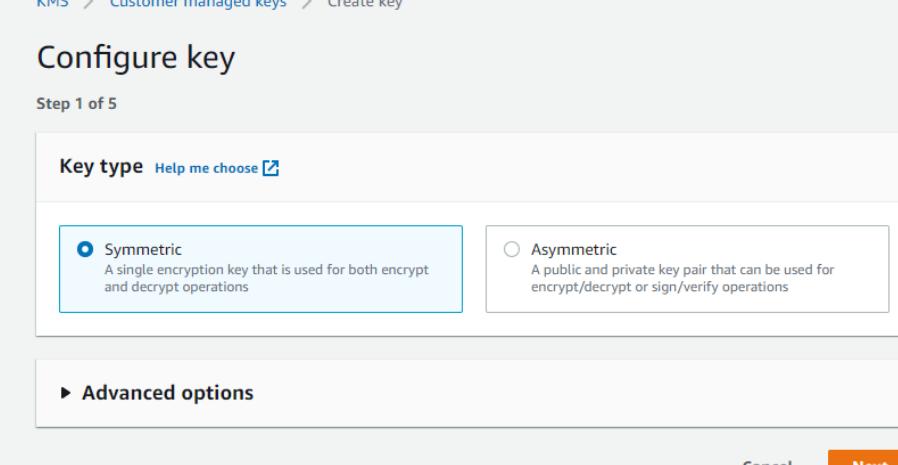
Key type [Help me choose](#)

Symmetric
A single encryption key that is used for both encrypt and decrypt operations

Asymmetric
A public and private key pair that can be used for encrypt/decrypt or sign/verify operations

Advanced options

Cancel Next



Key Management Service (KMS)

AWS managed keys Customer managed keys Custom key stores

Alias
You can change the alias at any time. [Learn more](#)

Alias
myFirstKey

Description - optional
You can change the description at any time.

Description - optional
KMS Key for S3 data

Tags - optional
You can use tags to categorize and identify your KMS keys and help you track your AWS costs. When you add tags to AWS resources, AWS generates a cost allocation report for each tag. [Learn more](#)

This key has no tags.

Add tag
You can add up to 50 more tags.

Cancel **Previous** **Next**

Key Management Service (KMS)

AWS managed keys Customer managed keys Custom key stores

KMS > Customer managed keys > Create key

Define key administrative permissions

Step 3 of 5

Key administrators
Choose the IAM users and roles who can administer this key through the KMS API. You may need to add additional permissions for the users or roles to administer this key from this console. [Learn more](#)

<input type="checkbox"/>	Name	Path	Type
<input checked="" type="checkbox"/>	awsstudent	/	User
<input type="checkbox"/>	AWSBatchServiceRole	/	Role
<input type="checkbox"/>	AWSServiceRoleForAmazonElasticsearchService	/aws-service-role/es.amazonaws.com/	Role
<input type="checkbox"/>	AWSServiceRoleForAPIGateway	/aws-service-role/ops.apigateway.amazonaws.com/	Role
<input type="checkbox"/>	AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling.amazonaws.com/	Role
<input type="checkbox"/>	AWSServiceRoleForAWSCloud9	/aws-service-role/cloud9.amazonaws.com/	Role
<input type="checkbox"/>	AWSServiceRoleForAWSLicenseManagerMasterAccountRole	/aws-service-role/license-manager.master-account.amazonaws.com/	Role

Screenshot of the AWS KMS console showing Step 4 of 5: Select IAM users and roles. The user 'awsstudent' is selected.

This account

Select the IAM users and roles that can use the KMS key in cryptographic operations. [Learn more](#)

Name	Path	Type
<input checked="" type="checkbox"/> awsstudent	/	User
<input type="checkbox"/> AWSBatchServiceRole	/	Role
<input type="checkbox"/> AWSServiceRoleForAmazonElasticsearchService	/aws-service-role/es.amazonaws.com/	Role
<input type="checkbox"/> AWSServiceRoleForAPIGateway	/aws-service-role/ops.apigateway.amazonaws.com/	Role
<input type="checkbox"/> AWSServiceRoleForAutoScaling	/aws-service-role/autoscaling.amazonaws.com/	Role
<input type="checkbox"/> AWSServiceRoleForAWSCloud9	/aws-service-role/cloud9.amazonaws.com/	Role
<input type="checkbox"/> AWSServiceRoleForAWSLicenseManagerMasterAccountRole	/aws-service-role/license-manager.master-account.amazonaws.com/	Role
<input type="checkbox"/> AWSServiceRoleForAWSLicenseManagerRole	/aws-service-role/license-manager.amazonaws.com/	Role
<input type="checkbox"/> AWSServiceRoleForDAX	/aws-service-role/dax.amazonaws.com/	Role

Screenshot of the AWS KMS console showing Step 4 of 5: Select IAM users and roles. The user 'awsstudent' is selected.

Key Management Service (KMS)

AWS managed keys

Customer managed keys

Custom key stores

myfirstkey

RMS Key for S3 data

Tags

Key	Value
No data	

No tags to display

Key policy

To change this policy, return to previous steps or edit the text here.

```
1 {
2     "Id": "key-consolepolicy-3",
3     "Version": "2012-10-17",
4     "Statement": [
5         {
6             "Sid": "Enable IAM User Permissions",
7             "Effect": "Allow",
8             "Principal": {
9                 "AWS": "arn:aws:iam::602742317511:root"
10            },
11            "Action": "kms:*",
12            "Resource": "*"
13        },
14        {
15            "Sid": "Allow access for Key Administrators",
16            "Effect": "Allow",
17            "Principal": "arn:aws:iam::602742317511:root",
18            "Action": "kms:DescribeKey",
19            "Resource": "arn:aws:kms:us-east-1:602742317511:key/1234abcd-1234-1234-1234-1234567890ab"
20        }
21    ]
22}
```

Cancel Previous **Finish**

The screenshot shows the AWS KMS (Key Management Service) console. On the left, there's a sidebar with navigation links: 'Key Management Service (KMS)', 'AWS managed keys', 'Customer managed keys' (which is highlighted in orange), and 'Custom key stores'. The main content area shows a key named '93945609-d2a3-46f1-837a-28694b1ea63f'. The 'General configuration' tab is selected, displaying details like Alias (myFirstKey), Status (Enabled), ARN (arn:aws:kms:us-west-2:602742317511:key/93945609-d2a3-46f1-837a-28694b1ea63f), Description (KMS Key for S3 data), Creation date (Dec 04, 2021 11:40 GMT+5:30), and Regionality (Single Region). Below this, tabs for 'Key policy', 'Cryptographic configuration', 'Tags', 'Key rotation', and 'Aliases' are visible. The 'Key policy' tab is active, showing a placeholder message: 'Choose the IAM users and roles who can administer this key through the KMS API. You might need to add additional permissions for the users or roles to administer this key in this console.' A 'Switch to policy' button is also present.

2. Configure CloudTrial to Store Logs in an S3 bucket

The screenshot shows the AWS search interface with the query 'cloudtrail' entered in the search bar. The left sidebar lists 'Key Management Service (KMS)' under 'Customer managed keys' and 'Custom key stores'. The main search results are categorized into 'Services' and 'Features'. Under 'Services', 'CloudTrail' is listed with the description 'Track User Activity and API Usage'. Under 'Features', 'AWS Transfer Family feature' is listed under 'Servers'. Other results like 'Detective' and 'Cloud9' are also shown.

The screenshot shows the AWS CloudTrail Management Console. The left sidebar includes links for Dashboard, Event history, Insights, Trails, Pricing, Documentation, Forums, and FAQs. The main content area displays three informational messages: 1) A blue banner at the top says "Now use IAM Access Analyzer on a CloudTrail trail" with a link to learn more. 2) A yellow warning message "Failed to get CloudTrail events" stating "You do not have permissions to perform this action. An administrator for your account might need to add permissions to the policy that grants you access to CloudTrail." 3) Another yellow warning message "Failed to get Insights events" with the same permission notice. Below these messages is a breadcrumb navigation path: CloudTrail > Dashboard. The dashboard itself has sections for "Trails" (listing one trail named "us-west-2-qtrail-lab-2481-1638597443" in a Logging status) and "CloudTrail Insights" (not enabled). There is also a "Event history" section.

The screenshot shows an AWS QwikLab session titled "An S3 Bucket". The top bar indicates the session is at 00:33:14. On the left, there's a "Caution" note about not deviating from lab instructions. A red "End Lab" button is visible. The main content area contains a numbered list of steps:

12. On the **Services** menu, click **CloudTrail**.
13. If you see the *New Event history features available in the new CloudTrail console* with **Try out the new console**, click **Try out the new console**, otherwise you can ignore this warning.
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.
15. If you see *You do not have permissions to perform this action. An administrator for your account might need to add permissions to the policy that grants you access to CloudTrail.*, you can ignore this warning.
16. In the navigation pane on the left, click **Trails**.
17. Click **Create trail** then configure:
 - Trail name: **myTrail**
 - Trail log bucket and folder: **mycloudtrailbucketNUMBER**
 - Replace **NUMBER** with a random number
 - De-select Log file SSE-KMS encryption
18. Click **Next**.

To the right of the main content is a sidebar with a table of contents for the lab, including sections like "Lab Overview", "Topics covered", "Prerequisites", "Start Lab", and various task steps. At the bottom, there's a Windows taskbar showing the date and time (11:44 AM 04-Dec-21).

S | Services | Search for services, features, blogs, docs, and more [Alt+S] | Oregon | awsstudent @ 6027-4231

CloudTrail X Now use IAM Access Analyzer on a CloudTrail trail
IAM Access Analyzer lets you implement least privilege permissions by generating IAM policies based on CloudTrail logs. [Learn more](#)

CloudTrail > Trails

Trails

Name	Home region	Multi-region trail	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
us-west-2-qtrail-lab-2481-1638597443	US West (Oregon)	No	Disabled	No	qtrail-lab-2481-1638597443			Logging

S | Services | Search for services, features, blogs, docs, and more [Alt+S] | Oregon

CloudTrail > Trails > Create trail

Step 1 Choose trail attributes

Step 2 Choose log events

Step 3 Review and create

Choose trail attributes

General details
A trail created in the console is a multi-region trail. [Learn more](#)

Trail name
Enter a display name for your trail.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Enable for all accounts in my organization
To review accounts in your organization, open AWS Organizations. [See all accounts](#)

Storage location [Info](#)

Create new S3 bucket
Create a bucket to store logs for the trail.

Use existing S3 bucket
Choose an existing bucket to store logs for this trail.

Trail log bucket and folder
Enter a new S3 bucket name and folder (prefix) to store your logs. Bucket names must be globally unique.

Logs will be stored in mycloudtrialbucket09/AWSLogs/602742317511

Log file SSE-KMS encryption [Info](#)

Enabled

Additional settings

The screenshot shows the AWS CloudTrail 'Create trail' wizard. The top navigation bar includes the AWS logo, 'Services' button, search bar ('Search for services, features, blogs, docs, and more'), and a help icon. A blue banner at the top says 'Now use IAM Access Analyzer on a CloudTrail trail' and 'IAM Access Analyzer lets you implement least privilege permissions by generating IAM policies based on CloudTrail logs. [Learn more](#)'. Below the banner, the breadcrumb path is 'CloudTrail > Trails > Create trail'. On the left, a sidebar shows three steps: 'Step 1 Choose trail attributes' (selected), 'Step 2 Choose log events' (current step), and 'Step 3 Review and create'. The main content area is titled 'Choose log events'. It has a sub-section 'Events Info' with a note about recording API activity for individual resources or all current and future resources in the account. It includes sections for 'Event type', 'Management events' (selected), 'Data events' (selected), and 'Insights events'. The 'Management events' section includes a note about capturing management operations performed on or within AWS resources.

The screenshot shows the AWS CloudTrail 'Create trail' wizard Step 2: 'Choose log events'. The top navigation bar and sidebar are identical to the previous screenshot. The main content area is titled 'Step 2: Choose log events' with an 'Edit' button. It contains three sections: 'Management events', 'Data events : S3 (1)', and 'Insights events'. The 'Management events' section shows settings for API activity (All) and excludes AWS KMS events (No). The 'Data events : S3 (1)' section shows a single entry for All current and future S3 buckets, with both Read and Write options set to Enabled. The 'Insights events' section is currently empty. At the bottom right are 'Cancel', 'Previous', and a large orange 'Create trail' button.

3. Upload an Image to your s3 bucket and encrypt it

The screenshot shows the AWS CloudTrail Management Console interface. A search bar at the top contains the query 's3'. The left sidebar has a 'CloudTrail' section and a 'Trails' section. The main content area displays search results for 's3' under three categories: Services, Features, and Datasets.

Services (7 results):

- S3: Scalable Storage in the Cloud. Sub-options: Buckets, Access points, Batch Operations.
- S3 Glacier: Archive Storage in the Cloud.
- Athena: Query Data in S3 using SQL.
- AWS Snow Family: Large Scale Data Transport.

Features (10 results):

- Amazon S3 File Gateway: Storage Gateway feature.

Datasets (1 result):

- IoT Analytics feature.

On the right side, there is a panel for managing CloudWatch Logs log groups, showing two entries: 'Status' and 'Logging'.

The screenshot shows the AWS S3 Management Console dashboard. On the left, a sidebar menu includes 'Buckets', 'Storage Lens', 'Feature spotlight', and 'AWS Marketplace for S3'. The main content area features a 'Account snapshot' section with metrics like Total storage (6.2 KB), Object count (1), and Avg. object size (6.2 KB). It also highlights 'AWS DataSync' and provides a 'View Storage Lens dashboard' button. Below this is a 'Buckets (3) Info' section with a table showing three buckets: 'mycloudtrialbucket09' (US West (Oregon) us-west-2), 'ql-cf-templates-1638597441-20bc1c7cdf10726e-us-west-2' (US West (Oregon) us-west-2), and 'qltrail-lab-2481-1638597443' (US East (N. Virginia) us-east-1).

This screenshot shows the 'Objects' tab for the 'mycloudtrialbucket09' bucket. The top navigation bar includes 'Feedback', 'English (US)', a search bar, and system icons. The main content area displays a table of objects, with one entry: 'AWSLogs/' which is a folder. Action buttons for 'Upload', 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', and 'Actions' are available above the table.

The screenshot shows the AWS S3 Management Console interface for uploading files. At the top, there are several browser tabs open, including 'Students study material shared', 'Students Study Material - Google', 'aws practical index with quick', 'Introduction to AWS Key Mana...', and 'S3 Management Console'. The main window is titled 'Upload' under 'Amazon S3 > mycloudtrialbucket09 > Upload'. A central message says, 'We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose Provide feedback.' Below this, a large text area says, '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'.

Upload Info

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.

Find by name

No files or folders

You have not chosen any files or folders to upload.

Destination

Feedback English (US) ▾ © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

A Windows file explorer window is overlaid on the S3 console, showing the file 'rose-165819_340' selected for upload. The file is located on the desktop and is a JPEG image (image/jpeg) with a size of 33.0 KB.

Open

This PC > Desktop >

Search Desktop

Organize New folder

Desktop Downloads Documents Pictures Chat CHFI RMI Windows 7 CF Eclipse IDE for Enterprise Java Developers... rose-165819_340

File name: rose-165819_340 Open Cancel

All files and folders in this table will be uploaded.

Find by name

rose-165819_340.jpg - image/jpeg 33.0 KB

Destination

Destination s3://mycloudtrialbucket09

Feedback English (US) ▾ © 2021, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

rose-165819_340.jpg Show all

Type here to search

Server-side encryption settings

Server-side encryption protects data at rest. [Learn more](#)

Server-side encryption

Do not specify an encryption key

Specify an encryption key

Encryption key type

To upload an object with a customer-provided encryption key (SSE-C), use the AWS CLI, AWS SDK, or Amazon S3 REST API.

Amazon S3 key (SSE-S3)
An encryption key that Amazon S3 creates, manages, and uses for you. [Learn more](#)

AWS Key Management Service key (SSE-KMS)
An encryption key protected by AWS Key Management Service (AWS KMS). [Learn more](#)

AWS KMS key

AWS managed key (aws/s3)
arn:aws:kms:us-west-2:602742317511:alias/aws/s3

Choose from your AWS KMS keys

Enter AWS KMS key ARN

AWS KMS key

arn:aws:kms:us-west-2:602742317511:key/93945... [Create key](#)

Bucket Key is disabled for objects uploaded, modified, or copied in this bucket

Uploaded, modified, or copied objects inherit their Bucket Key settings from the bucket default encryption configuration unless they already have Bucket Key configured. [Learn more](#)

Feedback English (US) ▾

Type here to search

End Lab 00:19:03

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](#)

24. From the Objects tab, click **Upload**

25. Click **Add files**

26. Browse to and select an image file on your computer

27. At the bottom of the screen, expand **Properties**.

28. In the **Server-side encryption settings** section, select **Specify an encryption key**

29. For **Encryption key type**, select **AWS Key Management Service key (SSE-KMS)**

30. For **AWS KMS key** Select **Choose from your AWS KMS keys**

31. From the drop down of the KMS master key, select *myFirstKey*

32. Scroll to the bottom of the screen, then click **Upload**

33. Click **Close** from the right corner of the **Upload: status** page.

34. Return to the bucket details by clicking the bucket name (as seen on the upper left)

35. Record the **Last modified** time to your text editor.

36. Return to the bucket details by clicking the bucket name (as seen on the upper left)

Lab Overview

Topics covered

Prerequisites

Start Lab

Task 1: Create Your KMS Master Key

Task 2: Configure CloudTrail to Store Logs In An S3 Bucket

Task 3: Upload an Image to Your S3 Bucket And Encrypt It

Task 4: Access The Encrypted Image

Task 5: Monitor KMS Activity Using CloudTrail Logs

Task 6: Manage Encryption Keys

End Lab

Conclusion

Additional Resources

The screenshot shows the AWS S3 Management Console interface. At the top, there are several tabs including "Students study material shared", "Students Study Material - Google Sheets", "aws practical index with quickstart", "Introduction to AWS Key Management Service", and "S3 Management Console". The main content area displays a success message: "Upload succeeded" with a link to "View details below." Below this, a summary table shows the destination as "s3://mycloudtrialbucket09" with one file uploaded successfully (33.0 KB) and no files failed. A "Close" button is in the top right corner of this summary box. Below the summary, there are two tabs: "Files and folders" (selected) and "Configuration". Under "Files and folders", a table lists one file: "rose-165819_340.jpg" (image/jpeg, 33.0 KB, Succeeded). The bottom of the screen shows the Windows taskbar with various pinned icons and the system clock indicating 12:00 PM on 04-Dec-21.

← Introduction to AWS Key Management Service



End Lab

00:03:33

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](#)

Task 6: Manage Encryption Keys

In this task you will manage encryption keys for users and roles.

63. On the **Services** menu, click **Key Management Service**.

64. Click **myFirstKey**.

On this page, you can alter the key's description, **Add** or **Remove** Key Administrators and Key Users, allow external users to access the key and place the key into annual rotation.

65. In the **Key users** section, select the user or role that you are signed in with.

66. Click the **Remove** button.

You have removed the user's permission to use this key.

67. In the **Key users** section, click the **Add** button then:

Lab Overview

Topics covered

Prerequisites

Start Lab

Task 1: Create Your KMS Master Key

Task 2: Configure CloudTrail to Store Logs In An S3 Bucket

Task 3: Upload an Image to Your S3 Bucket And Encrypt It

Task 4: Access The Encrypted Image

Task 5: Monitor KMS Activity Using CloudTrail Logs

Task 6: Manage Encryption Keys

End Lab

Apps sparkUI Mail - OmprakashY... Cox Communications Ambari jira jenkins Oozie Console Service Portal - Cox... TestCasesLocatn Jira

- Introduction to AWS Key Management Service

End Lab 00:03:12

Action: 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](#)

65. In the **Key users** section, select the user or role that you are signed in with.

66. Click the **Remove** button.

You have removed the user's permission to use this key.

67. In the **Key users** section, click the **Add** button then:

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

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

Lab Overview
Topics covered
Prerequisites
Start Lab
Task 1: Create Your KMS Master
Task 2: Configure CloudTrail to S...
In An S3 Bucket
Task 3: Upload an Image to Your...
And Encrypt It
Task 4: Access The Encrypted In...
Task 5: Monitor KMS Activity Usi...
CloudTrail Logs
Task 6: Manage Encryption Keys
End Lab

Practical No. 8

Case Study : Amazon Architecture

Aim: A) ABP News

B) Buzzdial

C) Classle

1. ABP News Case Study

ABP News is an Indian Hindi news channel owned by ABP Group. It is a free to air TV channel founded in 1998. It was formerly known as STAR News before being acquired by ABP Group.

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.

Challenges Faced by ABP.

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.

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.

- 1. Unfortunately, ANN’ existing managed service provider technology infrastructure could not meet these challenges.**
- 2. ANN could not gain the visibility to control and optimize its use of infrastructure resources.**
- 3. 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.**

Why Amazon Web Services

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).

In 2014, the company decided to migrate its infrastructure, applications, and services to AWS.

"We selected AWS because of the flexibility to align our infrastructure costs and consumption with demand, and the ease and simplicity with which we could move to the AWS Cloud," says Gondal. "AWS also specializes in infrastructure services that enable businesses like ours to distribute video content and mobile applications to users' smartphones, tablets, and personal computers."

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.

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.

ANN elected to use AWS Lambda to deliver an architecture that seamlessly updates content feeds served from Amazon S3 to mobile users without requiring the management and maintenance of a single server.

Key to ANN' success is its choice of AWS services to run its mobile applications.

Benefits.

- Using AWS has enabled ANN to support its increase in page views from 150 million to 500 million and accommodate sharp spikes in traffic with high performance when significant news events, including elections, occur.
- ANN has also successfully extended its portfolio of products and services from a single website to several websites, video content and a mobile application, since migrating to the AWS Cloud.
- Furthermore, through competitive pricing offered by AWS, including regular reductions and being able to pay only for the infrastructure resources used, ANN has been able to control costs and budget effectively.
- Using AWS has given ANN the confidence to evaluate using advanced tools such as machine learning and artificial intelligence to deliver on a range of new products.

2. Buzzdial Case Study

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.

The Challenge

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.

Why Amazon Web Services

Buzzdial selected Amazon Web Services (AWS) as a cloud service provider that could meet its needs. The business worked closely with AWS solution architects in New Zealand to determine the best architecture for its service. 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.

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.

The Benefits

- Buzzdial is now delivering a service that meets the demanding requirements of prominent broadcasters, brands, and rights-holders such as the Seven, Ten, and SBS television networks in Australia, ITV in Britain, the New Zealand Herald newspaper, and the All Blacks rugby union team.
- The caliber of clients and importance of its second-screen service to their businesses requires Buzzdial to undertake detailed monitoring and quality assurance processes.
- Buzzdial can provision resources to support hundreds of thousands of concurrent users coming onboard in a 10-minute period, and scale further if needed. If a customer conducts a broadcast event but fails to notify Buzzdial, the service provider can still scale in 10 to 15 minutes to support 10s of thousands of concurrent users.
- Buzzdial calculates that its capital and operating costs for infrastructure are 96 percent lower over two to three years than they would be with a physical infrastructure in a collocated data center.
- Buzzdial plans to add new AWS services in future as business grows.

3. Classle Case Study

Classle is 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. Classle, a social enterprise, is currently focusing on rural regions of India where students struggle with resource limitations.

Why Amazon Web Services

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.

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

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 53.

The Benefits

- Able to expand social learning platform globally
- Reduced webpage load times by 180 per cent
- Reduced time-to-market to just two days

