

AWS & Cloud Computing Project

Project: 1

Virtual Private Cloud

Create VPC with Public and Private Subnet and route table.

The screenshot shows the AWS VPC dashboard for a newly created VPC. A green success message at the top states: "You successfully created **vpc-0c4ae06a36fd8fc0e / myvpc1**". The main details section for the VPC includes:

VPC ID	State	Block Public Access	DNS hostnames
vpc-0c4ae06a36fd8fc0e	Available	Off	Disabled
DNS resolution	Tenancy	DHCP option set	Main route table
Enabled	default	dopt-09ceed705fc93fe53	rtb-07f0f644f040f6a22
Main network ACL	Default VPC	IPv4 CIDR	IPv6 pool
acl-0736279e80af84093	No	16.0.0.0/16	-
IPv6 CIDR	Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups	Owner ID
-	Disabled	-	225578988181
Encryption control ID	Encryption control mode		
-	-		

Below the details, there are tabs for "Resource map", "CIDRs", "Flow logs", "Tags", and "Integrations". The "Resource map" tab is selected, showing a summary of resources:

- VPC
- Subnets (0)
- Route tables (1)

A "Show all details" button is located in the bottom right corner of the resource map area.

Then, Create internet gateway for public subnet and NAT Gate for private subnet. Connect the route table.

The screenshot shows the AWS VPC dashboard with the 'NAT gateways' section selected. A success message at the top states: "NAT gateway nat-188aabcb9089569ac | mynatghate was created successfully." The main card displays the following details for the NAT gateway:

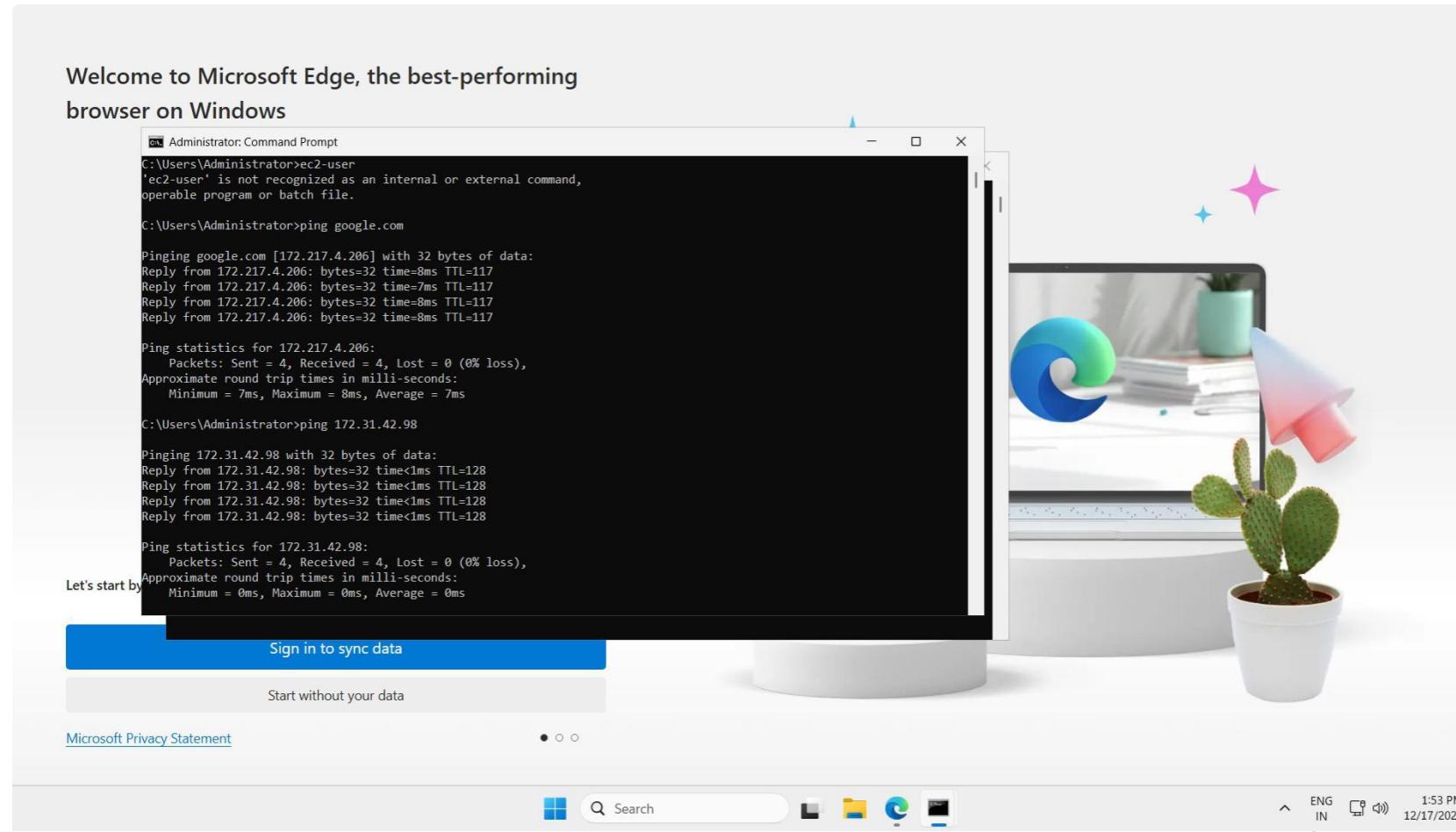
NAT gateway ID	Availability mode	State	State message
nat-188aabcb9089569ac	Regional	Pending	-
NAT gateway ARN	Connectivity type	Created	Deleted
arn:aws:ec2:us-east-2:225578988181:natgateway/nat-188aabcb9089569ac	Public	Wednesday, December 17, 2025 at 18:58:55 GMT+5:30	-
VPC	Method of EIP allocation	Actions	
vpc-0c4ae06a36fd8fc0e / myvpc1	Automatic	Edit Delete	

Below the details, there are tabs for "IP addresses", "Monitoring", "Flow logs", and "Tags". The "IP addresses" tab is active, showing a table titled "Associated IP addresses". The table has columns for "IP address", "Status", "Availability Zone", and "Allocation ID". A note below the table states: "No associated IP addresses found. If this NAT gateway was recently created with the automatic allocation method, your IP addresses are still being allocated. Click the refresh button to view them."

After create VPC create a public instance and connect the instance to RDP connect.

The screenshot shows the AWS EC2 Connect interface for a public instance (i-0b4174595d52aaaf13). The top navigation bar includes 'EC2 > Instances > i-0b4174595d52aaaf13 > Connect to instance'. The main tabs are 'Session Manager', 'RDP client' (which is selected), and 'EC2 serial console'. A callout box at the top left says 'Record RDP connections' and 'You can now record RDP connections using AWS Systems Manager just-in-time node access. [Learn more](#)'. On the right, there's a 'Try for free' button and a close 'X' button. The 'Instance ID' is listed as 'i-0b4174595d52aaaf13 (pubinstance1)'. Under 'Connection Type', 'Connect using RDP client' is selected, with a note: 'Download a file to use with your RDP client and retrieve your password.' To the right, 'Connect using Fleet Manager' is shown with a note: 'To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)'. Below these, a note says 'You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:'. A 'Download remote desktop file' button is available. The 'Public DNS' field contains 'ec2-18-222-147-39.us-east-2.compute.amazonaws.com'. A green message box says 'Password copied' with a clipboard icon. The 'Username' dropdown is set to 'Administrator'. At the bottom, a note says 'If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.'

After connected to RDP check the internet connection for public and private subnets. Once network is running our VPC done .
Finall output both connections are running.



Project : 2

- ▶ EC2 backup using snapshot and IAM

First create Instance

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections for EC2 (Dashboard, EC2 Global View, Events), Instances (Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Capacity Manager), Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes). The main content area displays the following information:

Instances (1/1) Info

- Last updated 4 minutes ago
- Connect
- Instance state ▾
- Actions ▾
- Launch instances ▾

Filter options include Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4. A search bar says "Find Instance by attribute or tag (case-sensitive)".

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
myinsg	i-094a369ee3870b82f	Running	t3.micro	3/3 checks passed	View alarms +	us-east-2c	ec2-3-17-2c

i-094a369ee3870b82f (myinsg)

Volume	Device	Size (GB)	Status	Attached	Created	Delete
vol-05b4afb6e204c8ebe	/dev/sda1	30	In-use	Attached	2025/12/18 10:37 GMT+5:30	No

Volume monitoring (1)

Alarm recommendations: Investigate with AI - new 3h 1d 1w 1h UTC timezone Connect Explore related

Metrics shown: Stalled I/O Check, Average read latency (ms/op), Average write latency (ms/op), Read throughput (KiB/s).

Then, create snapshot for instance and create column for snapshot. Then attach the column to instance. If the volume is deleted automatically backup volume.

The screenshot shows the AWS EBS Volumes page. On the left, a navigation sidebar lists various services: Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Capacity Manager (New), Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), and Load Balancing (Load Balancers). The main content area displays two volumes:

Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot ID	Source volume ID	Created
vol-09f8eedc9dc874ff3	vol-09f8eedc9dc874ff3	gp3	30 GiB	3000	125	snap-0f22d0f...	-	2025/12/18
vol-05b4afb6e204c8ebe	vol-05b4afb6e204c8ebe	gp3	30 GiB	3000	125	snap-0c9c090...	-	2025/12/18

Below the table, a specific volume is selected (vol-09f8eedc9dc874ff3), and its details are shown in a modal window:

Volume ID: vol-09f8eedc9dc874ff3			
Details			
Volume ID vol-09f8eedc9dc874ff3	Size 30 GiB	Type gp3	Status check Okay
AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more	Volume state Available	IOPS 3000	Throughput 125
Fast snapshot restored No	Availability Zone use2-az1 (us-east-2a)	Created Thu Dec 18 2025 10:48:18 GMT+0530 (India Standard Time)	Multi-Attach enabled No

- Next we create a backup for whole instance using IAM.
Create IAM for instance backup. If the instance delete them automatically backup the whole instance.

Instances (1/2) Info

Last updated less than a minute ago

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
myinsg	i-094a369ee3870b82f	Running	t3.micro	3/3 checks passec	View alarms +	us-east-2c	ec2-3-17-20
myins18backup	i-0626c3d41ac557589	Running	t3.micro	3/3 checks passec	View alarms +	us-east-2c	ec2-52-14-2

i-0626c3d41ac557589 (myins18backup)

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary

Instance ID i-0626c3d41ac557589	Public IPv4 address 52.14.235.121 open address ↗	Private IPv4 addresses 172.31.32.249
IPv6 address -	Instance state Running	Public DNS ec2-52-14-235-121.us-east-2.compute.amazonaws.com open address ↗

Project 3: Motoring Service

- ▶ Set Alarm for S3 bucket using Cloudwatch

- First we create s3 bucket.
Next create loggroup for putobject on s3 bucket using cloudwatch.
Then create cloudtrail for that loggroup.

CloudTrail > Trails > arn:aws:cloudtrail:us-east-2:225578988181:trail/mytrails3

mytrails3

General details

Trail logging	<input checked="" type="checkbox"/> Logging
Trail name	mytrails3
Multi-region trail	Yes
Apply trail to my organization	Not enabled
Trail log location	aws-cloudtrail-logs-225578988181-e7c10cda/AWSLogs/225578988181
Last log file delivered	-
Log file SSE-KMS encryption	Not enabled
Log file validation	Disabled
Last file validation delivered	-
SNS notification delivery	Disabled
Last SNS notification	-

CloudWatch Logs

Log group	s3bucket
IAM Role	arn:aws:iam::225578988181:role/service-role/s3rule

Tags

Key	Value
-----	-------

- Next set Cloudwatch alarm for putobject on s3 bucket. Create topic and subscribe the notification Receive.

Amazon SNS > Topics > mys3topic > Subscription: 06787463-1efe-48c6-8896-7bc9df4e97b1

Subscription: 06787463-1efe-48c6-8896-7bc9df4e97b1

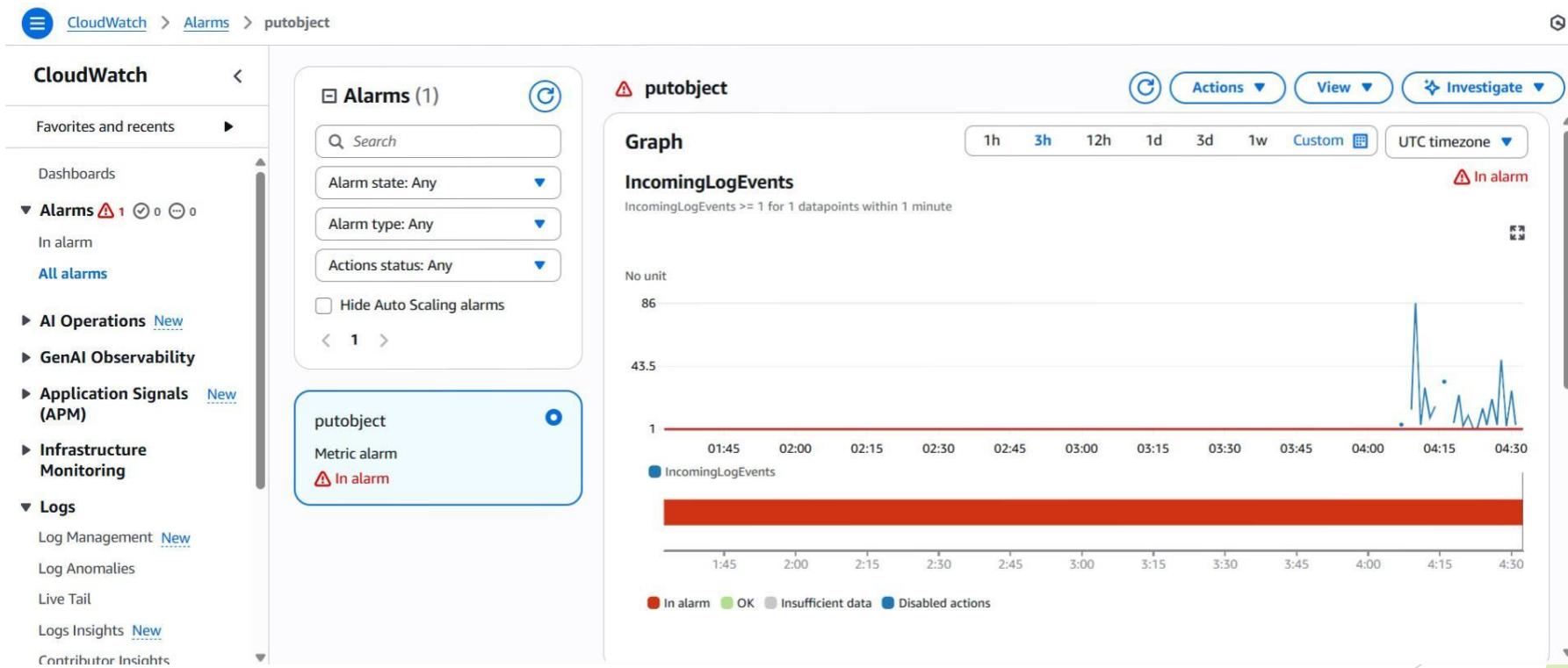
Details

ARN	<input type="checkbox"/> arn:aws:sns:us-east-2:225578988181:mys3topic:06787463-1efe-48c6-8896-7bc9df4e97b1
Endpoint	gayumachlm@gmail.com
Topic	mys3topic
Subscription Principal	arn:aws:iam::225578988181:root
Status	<input checked="" type="checkbox"/> Confirmed
Protocol	EMAIL

[Subscription filter policy](#) [Redrive policy \(dead-letter queue\)](#)

Subscription filter policy Info
This policy filters the messages that a subscriber receives.

- Next select the metrics filter in Cloudwatch. Then put the object on s3 bucket. Once the Cloudwatch graph is cross the limit we received the notification mail.



- Finally the mail is received to our given mail id.

Gmail Search mail

Compose

Inbox 6

Starred Snoozed Sent Drafts 1 Purchases More

Labels +

ALARM: "putobject" in US East (Ohio) Inbox x

AWS Notifications <no-reply@sns.amazonaws.com> to me 10:03 AM (0 minutes ago)

You are receiving this email because your Amazon CloudWatch Alarm "putobject" in the US East (Ohio) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [87.0 (18/12/25 04:32:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Thursday 18 December, 2025 04:33:17 UTC".

View this alarm in the AWS Management Console:
<https://us-east-2.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-2#alarmsV2:alarm/putobject>

Alarm Details:

- Name: putobject
- Description: your s3 bucket received on object
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [87.0 (18/12/25 04:32:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Thursday 18 December, 2025 04:33:17 UTC
- AWS Account: 225578988181
- Alarm Arn: arn:aws:cloudwatch:us-east-2:225578988181:alarm:putobject

Threshold:

- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0 for at least 1 of the last 1 period(s) of 60 seconds.

Monitored Metric:

- MetricNamespace: AWS/Logs

Enable desktop notifications for Gmail. **OK** **No thanks** **X** **Forward** **Smile**

Project 4: Notification Services

- ▶ Simple Notification Service(SNS)
- ▶ Set Notification for cpu utilisation alert

- Open SNS, then create topic for cpu utilisation.

The screenshot shows the Amazon SNS Topics page. In the top left, the navigation path is "Amazon SNS > Topics > cpualert". On the left sidebar, under "Amazon SNS", there are links for Dashboard, Topics (which is selected and highlighted in blue), Subscriptions, and Mobile (Push notifications and Text messaging (SMS)).

A prominent blue banner at the top right indicates a "New Feature": "Amazon SNS now supports High Throughput FIFO topics. [Learn more ↗](#)". Below this, a green success message states "Topic cpualert created successfully. You can create subscriptions and send messages to them from this topic." with a "Publish message" button.

The main content area shows the details for the "cpualert" topic. The "Details" section includes:

- Name: cpualert
- ARN: arn:aws:sns:us-east-2:22557898 8181:cpualert
- Display name: -
- Type: Standard

The "Topic owner" is listed as 225578988181.

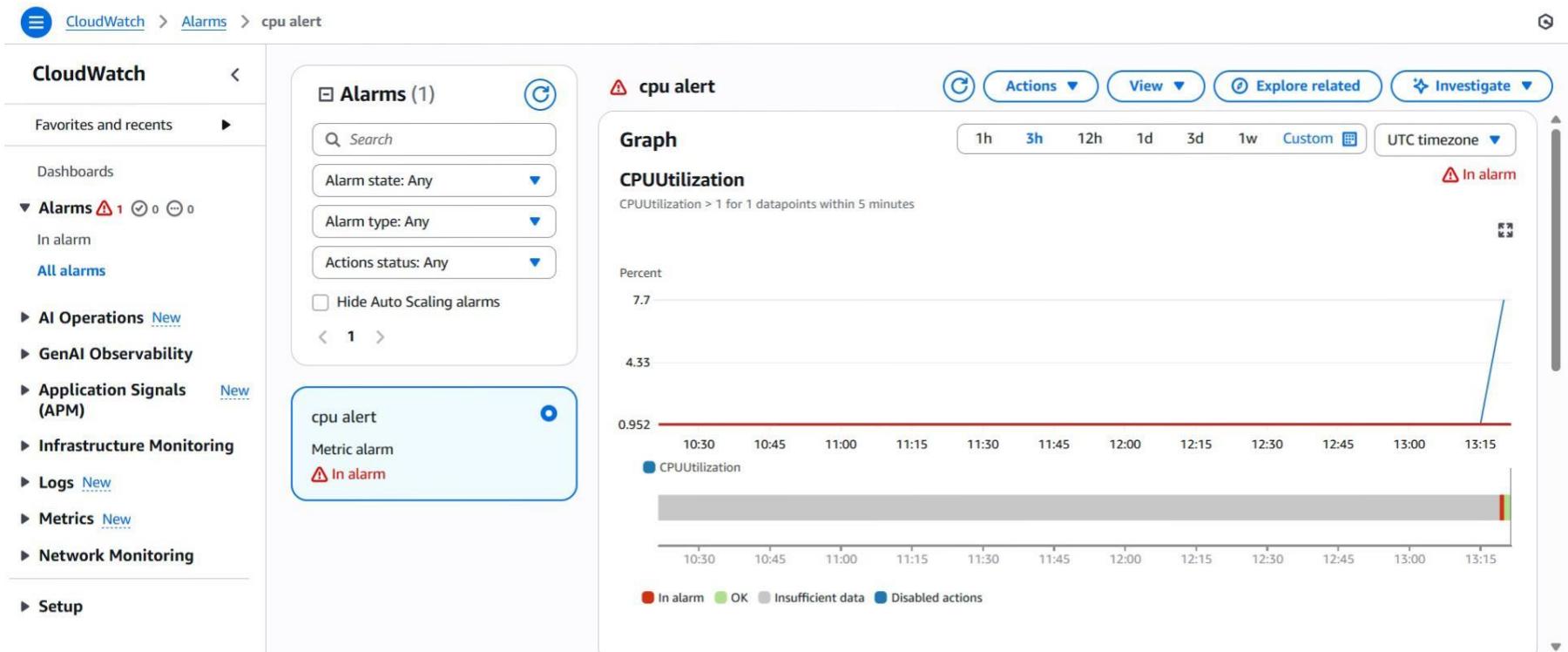
The navigation tabs below the details are: Subscriptions (selected), Access policy, Data protection policy, Delivery policy (HTTP/S), Delivery status logging, Encryption, and Tags.

The "Subscriptions" tab shows a table with one row, indicating 0 subscriptions. The table includes columns for "Edit", "Delete", "Request confirmation", "Confirm subscription", and a yellow "Create subscription" button. A search bar is also present.

- Then create subscription for alert and confirm subscription.

The screenshot shows the Amazon SNS console with the URL [Amazon SNS > Topics > cpualert > Subscription: 62f5ed3f-9111-4360-adb6-8cff4bf10b33](#). The left sidebar has 'Subscriptions' selected under 'Topics'. The main area displays a 'Subscription: 62f5ed3f-9111-4360-adb6-8cff4bf10b33' card. The card includes fields for ARN (arn:aws:sns:us-east-2:225578988181:cpualert:62f5ed3f-9111-4360-adb6-8cff4bf10b33), Endpoint (gayuselvasathy@gmail.com), Topic (cpualert), Status (Confirmed), and Protocol (EMAIL). Below the card are tabs for 'Subscription filter policy' (selected) and 'Redrive policy (dead-letter queue)'. A note at the bottom states: 'This policy filters the messages that a subscriber receives.'

- Once the CPU utilisation is cross the limit, the graph will cross the line and alarm status change to In-alarm.



- Then, we received the alert mail to our given mail id.

The screenshot shows a Gmail inbox with the following details:

- Inbox:** The selected folder.
- Compose:** Button for composing a new email.
- AWS Notifications <no-reply@sns.amazonaws.com>**: The sender of the email.
- Subject:** ALARM: "cpu alert" in US East (Ohio)
- Date:** 6:49 PM (3 minutes ago)
- Email Content:**
 - You are receiving this email because your Amazon CloudWatch Alarm "cpu alert" in the US East (Ohio) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [1.1436769026612648 (13/12/25 13:14:00)] was greater than the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Saturday 13 December, 2025 13:19:08 UTC".
 - View this alarm in the AWS Management Console:** <https://us-east-2.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-2#alarmsV2.alarm/cpu%20alert>
 - Alarm Details:**
 - Name: cpu alert
 - Description:
 - State Change: INSUFFICIENT_DATA -> ALARM
 - Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [1.1436769026612648 (13/12/25 13:14:00)] was greater than the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).
 - Timestamp: Saturday 13 December, 2025 13:19:08 UTC
 - AWS Account: 225578988181
 - Alarm Arn: arn:aws:cloudwatch:us-east-2:225578988181:alarm:cpu alert
 - Threshold:**
 - The alarm is in the ALARM state when the metric is GreaterThanThreshold 1.0 for at least 1 of the last 1 period(s) of 300 seconds.
 - Monitored Metric:**
 - MetricNamespace: AWS/EC2
 - MetricName: CPUUtilization
 - Dimensions: [InstanceId = i-0045a5c210758290f]
 - Period: 300 seconds
 - Statistic: Average

- Simple Queue Service(SQS)

- Create SQS for message. This message is received to customer, the customer view the message when we have time.

The screenshot shows the AWS SQS Queue Details page for a queue named 'myqueue'. The queue is of type 'Standard' and has an ARN of 'arn:aws:sqs:us-east-2:225578988181:myqueue'. It includes an 'Encryption' section using an 'Amazon SQS key (SSE-SQS)'. The 'URL' for the queue is provided. A 'Dead-letter queue' section is present but empty. Below the details, there are tabs for 'Queue policies', 'Monitoring', 'SNS subscriptions', 'Lambda triggers', 'EventBridge Pipes', 'Dead-letter queue', 'Tagging', 'Encryption', and 'Dead-letter queue redri...'. The 'Queue policies' tab is currently selected. Under 'Access policy', it says 'Define who can access your queue.' and shows the following JSON policy:

```
{
  "Version": "2012-10-17",
  "Id": "__default_policy_ID",
  "Statement": [
    {
      "Sid": "owner_statement"
    }
  ]
}
```

- Set message in send message column.
Type the message what receive to client.

The screenshot shows the AWS SQS 'Send and receive messages' interface. At the top, there's a navigation bar with the AWS logo, search bar, and account information (Account ID: 2255-7898-8181). Below the navigation, the URL is [Amazon SQS > Queues > myqueue > Send and receive messages](#). A message states: "Use this page to send, retrieve and view messages, helping you experiment with various queue features." The main area is titled "Send message" with an "Info" link. A green success message box contains the text: "Your message has been sent and is ready to be received." To the right of this box are "View sent message details" and a close "X" button. Below this, the "Message body" section contains the text: "your s3 bucket object storage is cross the limit." The "Message group ID - optional, new" section is present but empty. The "Delivery delay" section shows a value of "0" in seconds. The "Message attributes - optional" section is collapsed. At the bottom right are "Clear content" and "Send message" buttons.

aws | Search [Alt+S] Account ID: 2255-7898-8181 gayathri%20s

☰ Amazon SQS > Queues > myqueue > Send and receive messages

Use this page to send, retrieve and view messages, helping you experiment with various queue features.

Send message [Info](#)

✓ Your message has been sent and is ready to be received. [View sent message details](#) X

Message body
Enter the message to send to the queue.
your s3 bucket object storage is cross the limit.

Message group ID - optional, new [Info](#)
A group identifier for the message to allow fair processing across message groups in a standard queue.

Message group ID must be 1 to 128 characters. Valid characters are a-z, A-Z, 0-9, and punctuation (!#\$%&'()*+,-./;<=>?@[\\]^_`{}~-).

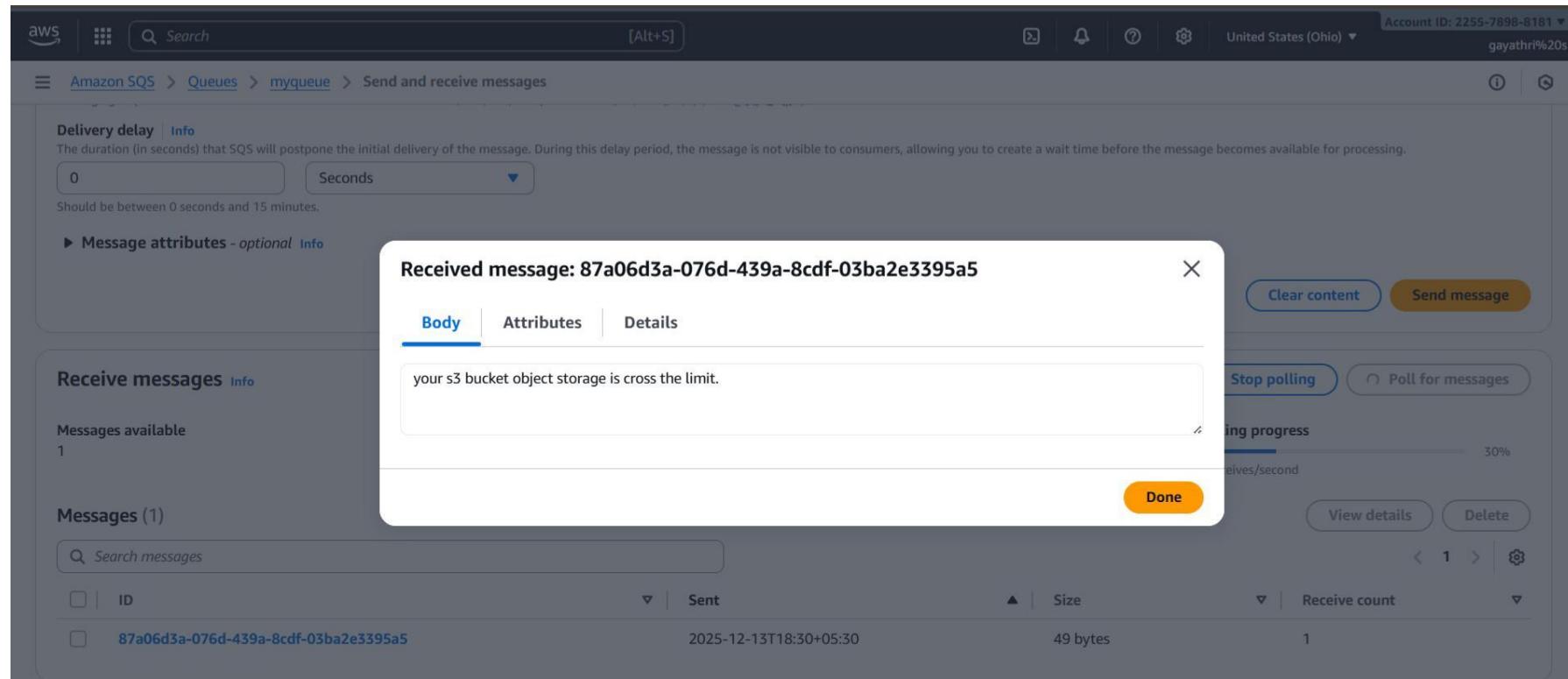
Delivery delay [Info](#)
The duration (in seconds) that SQS will postpone the initial delivery of the message. During this delay period, the message is not visible to consumers, allowing you to create a wait time before the message becomes available for processing.

0 Seconds ▾
Should be between 0 seconds and 15 minutes.

▶ **Message attributes - optional** [Info](#)

[Clear content](#) [Send message](#)

- When we have time click the poll for messages , the message will be show for 30sec. The message will disappear after 30sec. Again we want to read again click the poll for messages.



Project : 5

- ▶ Storage Service(S3 Bucket)

- Create ah S3 bucket with Unique Name and ACL enable with public access.

The screenshot shows the AWS S3 Buckets page. At the top, there's a green success message: "Successfully created bucket 'gayulithu'. To upload files and folders, or to configure additional bucket settings, choose View details." Below this, there are two tabs: "General purpose buckets" (selected) and "All AWS Regions". On the left, there's a search bar and a "Create bucket" button. The main area displays a table for "General purpose buckets (1/1)". The table has columns for "Name", "AWS Region", and "Creation date". One row is shown, with "Name" set to "gayulithu", "AWS Region" set to "US East (Ohio) us-east-2", and "Creation date" set to "December 13, 2025, 19:30:47 (UTC+05:30)". There are also buttons for "Copy ARN", "Empty", and "Delete". To the right of the table, there are two cards: "Account snapshot" (updated daily) and "External access summary - new" (updated daily).

Name	AWS Region	Creation date
gayulithu	US East (Ohio) us-east-2	December 13, 2025, 19:30:47 (UTC+05:30)

- Then, Upload any object in bucket (like images,songs,videos etc..) I upload the resume document. Give grand permission for object. For use of we access anywhere.

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and account information (Account ID: 2255-7898-8181, gayathri%20s). Below the navigation bar, a green success message box displays "Upload succeeded" and "For more information, see the Files and folders table." A note below it says "After you navigate away from this page, the following information is no longer available." The main area is titled "Summary" and shows upload statistics: "Destination s3://gayulithu", "Succeeded 1 file, 35.6 KB (100.00%)", and "Failed 0 files, 0 B (0%)". There are two tabs at the bottom: "Files and folders" (which is selected) and "Configuration". The "Files and folders" section shows a table with one item: "Amazon_S3_Seminar_PPT.pptx" (Type: application/vnd.openxmlform..., Size: 35.6 KB, Status: Succeeded). A "Find by name" search bar is also present in this section.

- Then open the upload page copy the URL for the object. Paste in new browser the file will be download to our device.

