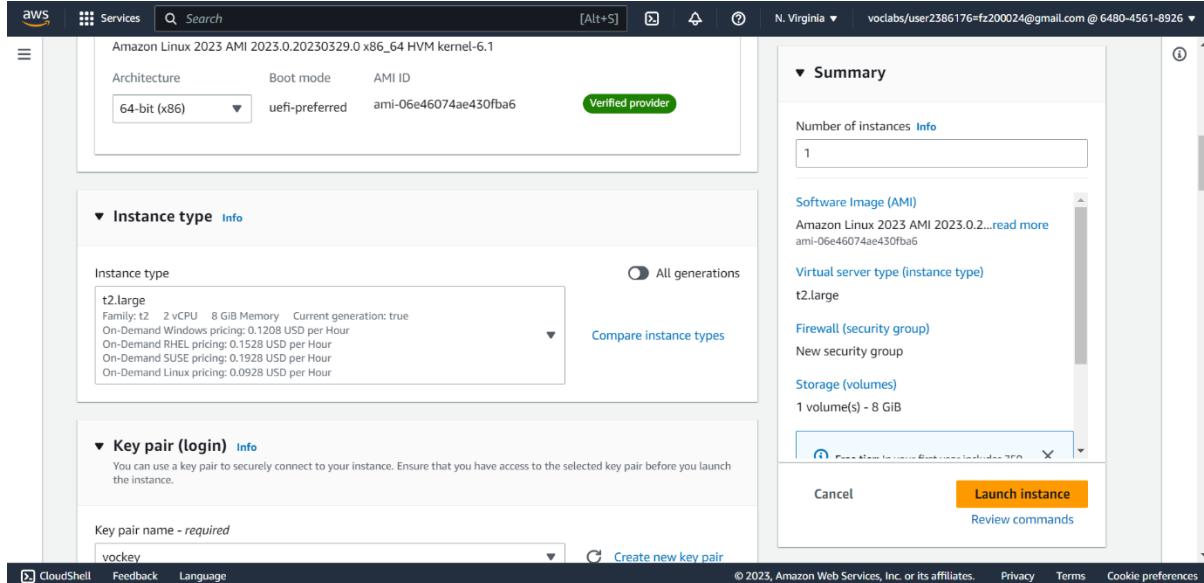
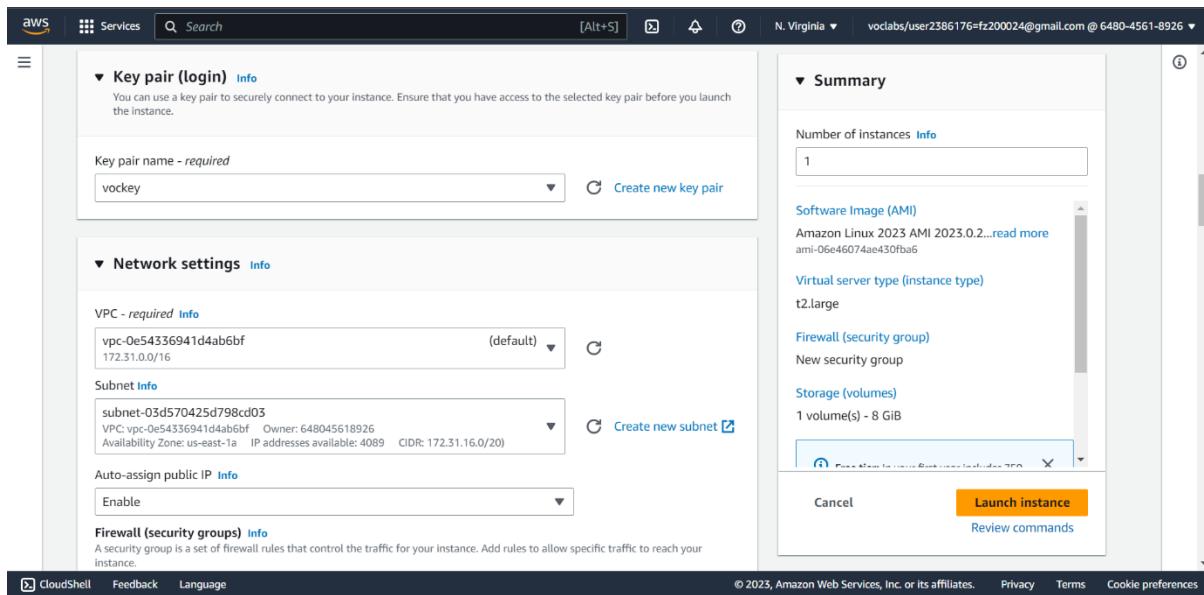


PART A:

To begin the creation of the three-server load-balanced system, three instances of the EC2 server, namely EC2 Server 1, EC2 Server 2 and EC2 Server 3 are first to be created with the t2.large instance type being dual-core with 8GBs of RAM.



Since all three servers need to be in separate availability zones, each of them are assigned to the zones, us-east-1a, us-east-1b, & us-east-1c respectively through the subnet drop-down list.



In the user data text field, the following HTML code is entered for the server to be able to display HTML pages that indicate their names for each page (given is only for EC2 Server 1, text for the server number is changed according to the server name in which website is being added)

```
#!/bin/bash
yum update -y
yum -y install httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>EC2 Server 1</h1></html>' > /var/www/html/index.html
```

User data has already been base64 encoded

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.0.2... [read more](#)

Virtual server type (instance type): t2.large

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

[Launch instance](#) [Review commands](#)

The three EC2 instances have been created

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
EC2 Server 2	i-0c088816bf97e75c0	Running	t2.large	2/2 checks passed	No alarms	us-east-1b	ec2-54-225-10-134.co...	54.225.10.134
EC2 Server 1	i-0280af342af40dc1e	Running	t2.large	2/2 checks passed	No alarms	us-east-1a	ec2-50-15-164-72.com...	50.16.164.72
EC2 Server 3	i-0b30f3ae8bdbeabd6	Running	t2.large	2/2 checks passed	No alarms	us-east-1c	ec2-3-215-80-98.comp...	3.216.80.98

After creation of the three EC2 instances, on the left panel under the Network and Security, in the Security Groups page, the three new security policies that were created upon the creation of the EC2 instances are each modified to be of type HTTP that allow for any and all inbound IPv4 addresses and traffic to reach the instance. This makes the website in the instance public for everyone to view.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sg-0c4411f9fb9bd4f23	HTTP	TCP	80	Custom	0.0.0.0 X

[Add rule](#) [Cancel](#) [Preview changes](#) [Save rules](#)

Following is the result of accessing each instance's respective websites by pasting their respective public IP address into the browser search bar:

The screenshot shows the AWS EC2 Instances page with three instances listed:

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 IP
EC2 Server 2	i-0cd88816bf97e75c0	Running	t2.large	2/2 checks passed	No alarms	us-east-1b	ec2-54-162-13-125.co...	54.162.13.125
EC2 Server 1	i-0280af342af40dc1e	Running	t2.large	2/2 checks passed	No alarms	us-east-1a	ec2-54-236-66-191.co...	54.236.66.191
EC2 Server 3	i-0b38f3ae8bdbeabd6	Running	t2.large	2/2 checks passed	1 alarms	us-east-1c	ec2-3-237-177-206.co...	3.237.177.206

Below the table, the details for EC2 Server 1 are shown:

- Public IPv4 address:** 54.236.66.191 | [open address](#)
- Public IPv4 DNS:** ec2-54-236-66-191.compute-1.amazonaws.com | [open address](#)

Three browser windows below show the results of visiting these addresses:

- EC2 Server 1:** Public IP 23.21.31.229
- EC2 Server 2:** Public IP 75.101.193.79
- EC2 Server 3:** Public IP 3.237.232.140

Now, three EBS Volumes by the name of EBS Volume 1, EBS Volume 3.1, and EBS Volume 3.2 are created with each volume having 10GBs of Magnetic (standard) storage each. The volumes are assigned different availability zones based on the EC2 instance that they are to be attached to. For EBS Volume 1, availability zone is configured as us-east-1a since it will be attached to EC2 Server 1, whereas for EBS Volume 3.1 and 3.2, the availability zone is configured as us-east-1c for both since they will both be attached to EC2 Server 3.

The screenshot shows the AWS Create volume page with the following settings:

- Volume settings**
- Volume type:** Magnetic (standard)
- Size (GiB):** 10
- IOPS:** Not applicable
- Throughput (MiB/s):** Not applicable
- Availability Zone:** us-east-1a

Next, an Elastic Load Balancer is to be created to handle the traffic load for the three servers, from the Load Balancers page that is accessed from the EC2 left hand pane. An application load balancer is chosen to be created, because this load balancer service is specifically designed for being capable of distributing incoming traffic across multiple targets, including EC2 instances. Considering that in this case EC2 instances have been used for server creation and static website hosting, an Application Load Balancer is the best choice in this scenario.

The screenshot shows the AWS Management Console with the URL [https://console.aws.amazon.com/ec2/v2/home?#/loadBalancers](#). The top navigation bar includes 'Services' and a search bar. The main content area is titled 'Select load balancer type'. It features three cards:

- Application Load Balancer**: Handles HTTP and HTTPS traffic with ALB, VPC, and target groups.
- Network Load Balancer**: Handles TCP, UDP, and TLS traffic with NLB, VPC, and target groups.
- Gateway Load Balancer**: Handles traffic for third-party virtual appliances with GWLB, VPC, and target groups.

Below each card is a brief description of its purpose and target applications.

The load balancer is assigned a name **myloadbalancer** and the three availability zones of the EC2 instances EC2 Server 1, EC2 Server 2 and EC2 Server 3.

The screenshot shows the 'Create Application Load Balancer' configuration page. The URL is [https://console.aws.amazon.com/ec2/v2/home?#/loadBalancers/create](#). The page has sections for 'Basic configuration' and 'How Elastic Load balancing works'. In 'Basic configuration', the 'Load balancer name' is set to 'myloadbalancer'. The 'Scheme' section shows 'Internet-facing' is selected. The 'IP address type' section shows 'IPv4' is selected. The 'IP address allocation' section shows 'Dualstack' is selected.

Network mapping [Info](#)

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC [Info](#)
Select the virtual private cloud (VPC) for your targets. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

- vpc-0e5433981d4ab6bf
IPv4: 172.31.0.0/16

Mappings [Info](#)
Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

us-east-1a (use1-az4)

Subnet

IPv4 settings
Assigned by AWS

us-east-1b (use1-az6)

Subnet

IPv4 settings
Assigned by AWS

us-east-1c (use1-az1)

Subnet

[CloudShell](#) [Feedback](#) [Language](#)

N. Virginia v vodabs/user2386176-fz200024@gmail.com @ 6480-4561-8926 v

© 2023, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Security groups [Info](#)

A security group is a set of firewall rules that control the traffic to your load balancer.

Security groups

VPC: vpc-0e5433981d4ab6bf

[CloudShell](#) [Feedback](#) [Language](#)

N. Virginia v vodabs/user2386176-fz200024@gmail.com @ 6480-4561-8926 v

© 2023, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

A target group with the name of **myTG** is created to be added a listener for the load balancer.

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration
Settings in this section cannot be changed after the target group is created.

Choose a target type

Instances

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

IP addresses

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice-based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

Lambda function

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

Application Load Balancer

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol :
Port

VPC
Select the VPC with the instances that you want to include in the target group.

[CloudShell](#) [Feedback](#) [Language](#)

N. Virginia v vodabs/user2386176-fz200024@gmail.com @ 6480-4561-8926 v

© 2023, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Sep 1
Specify target group
Step 2
Register targets

Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (3/3)						
<input checked="" type="checkbox"/> Instance ID	Name	State	Security groups	Zone	Subnet ID	
i-0c088816bf97e75c0	EC2 Server 2		launch-wizard-2	us-east-1b	subnet-0f440460cf544123d	
i-0280af542af40dc1e	EC2 Server 1		launch-wizard-1	us-east-1a	subnet-05d570425d798cd03	
i-0b38f3ae8bdbeabd6	EC2 Server 3		launch-wizard-3	us-east-1c	subnet-08ffcf1f55a326e22d	

3 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.
80
1-65535 (separate multiple ports with commas)

New EC2 Experience
Tell us what you think

EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances

Target groups (1) Info

<input type="checkbox"/> Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
myTG	arn:aws:elasticloadbalancing:us-east-1:648045618926:targetgroup/myTG/0e54336941d4ab6bf	80	HTTP	Instance	myloadbalancer	vpc-0e54336941d4ab6bf

Note: I forgot to screenshot this screen when initially selecting the target group, so I'm just showing the reselection again for the already selected target group which is why it is greyed out.

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

Listener HTTP:80

Protocol	Port	Default action
HTTP	:80	Forward to <input type="text" value="Select a target group"/> <input type="button" value="Create target"/>

Listener tags - optional
Consider adding tags to your listener. Tags enable you to categorize your AWS resources.

You can add up to 50 more tags.

Add-on services - optional
Additional AWS services can be integrated with this load balancer at launch. You can also add these and other services after your load balancer is created by reviewing the "Integrated services" section of the Load Balancer console.

The load balancer has been created and is tested out with the following results after refreshing every couple of times:

The screenshot shows the AWS EC2 Load Balancers console. On the left, there's a sidebar with options like New EC2 Experience, EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances, Instance Types, and Launch Templates. The main area displays a table titled 'Load balancers (1)'. The table has columns for Name, DNS name, State, VPC ID, Availability Zones, Type, Date created, and Instance ID. One row is shown: 'myloadbalancer' with 'myloadbalancer-1182819057.us-east-1.elb.amazonaws.com' as the DNS name, 'Active' status, 'vpc-0e54336941d4ab6bf' VPC, '3 Availability Zones', 'application' type, and 'April 12, 2023, 01:21 (UTC+04:00)' as the date created.

This screenshot shows the 'Details' page for the 'myloadbalancer' load balancer. It includes sections for Load balancer type (Application), IP address type (IPv4), Scheme (Internet-facing), Availability Zones, and Hosted zone. Below this, there are tabs for Listeners, Network mapping, Security, Monitoring, Integrations, Attributes, and Tags. The 'Listeners' tab is selected, showing a table with one entry: 'HTTP:80' with 'Not applicable' for both ARN and Security policy. A red box highlights the 'Default routing rule' section, which contains a single rule: 'Forward to myTG 1 (100%)' with 'Group-level stickiness: Off'.

Results:

Three browser tabs are shown, each displaying the URL 'myloadbalancer-1182819057.us-east-1.elb.amazonaws.com'. The tabs are labeled 'EC2 Server 2', 'EC2 Server 1', and 'EC2 Server 3'. Each tab shows a different web page content, indicating that the load balancer is distributing traffic to three different EC2 servers.

An alarm service is to be created now for monitoring the estimated charge of EC2. First, an SNS (Simple Notification Service) Topic by the name of MoneyAlert is created.

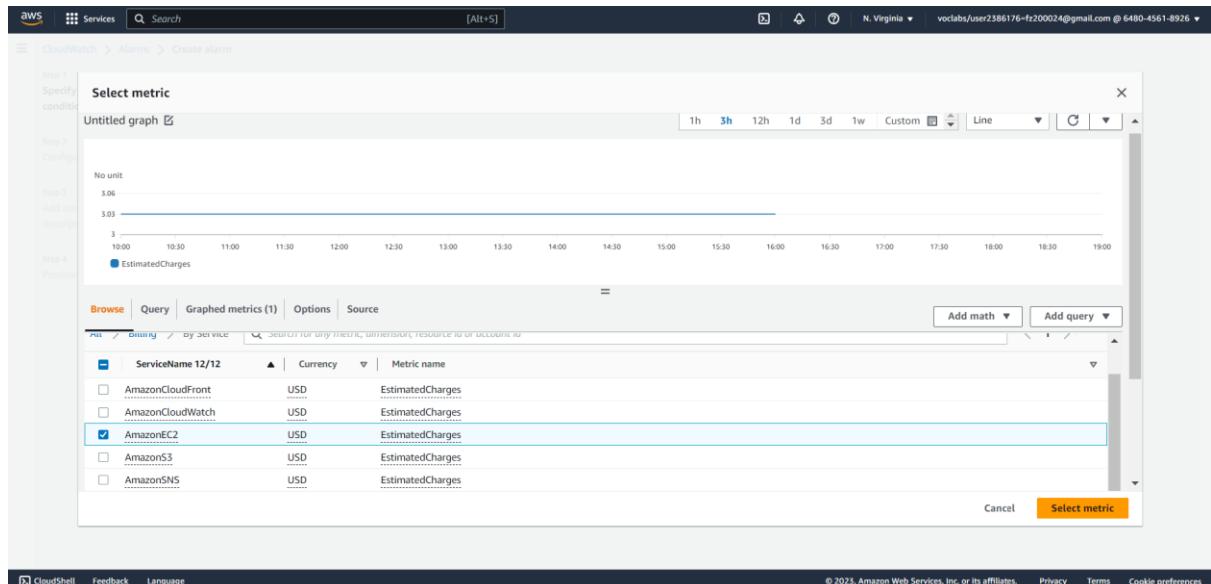
The screenshot shows the AWS Amazon SNS Topics console. On the left, there's a sidebar with options like Dashboard, Topics, Subscriptions, Mobile, and Push notifications. The main area displays a table titled 'Topics (2)'. The table has columns for Name, Type, and ARN. One row is shown: 'MoneyAlert' with 'Standard' Type and 'arn:aws:sns:us-east-1:648045618926:MoneyAlert' as the ARN.

Then a subscription for the MoneyAlert topic is created using the SMS protocol, and a verified phone number.

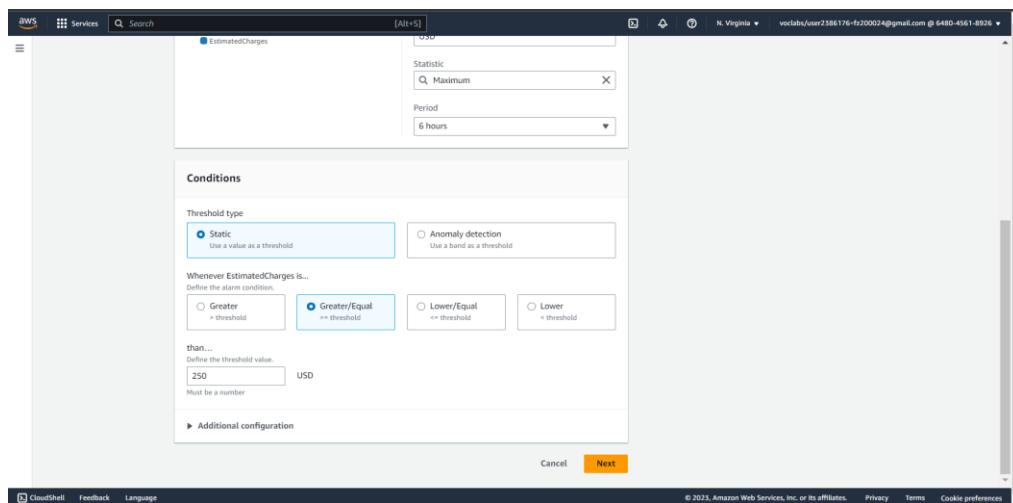
The screenshot shows the 'Create subscription' wizard in the AWS SNS console. The 'Details' step is selected. The 'Topic ARN' field contains 'arn:aws:sns:us-east-1:648045618926:MoneyAlert'. The 'Protocol' dropdown is set to 'SMS'. The 'Endpoint' field contains '+971552678219'. Below the form, there are two optional sections: 'Subscription filter policy' and 'Redrive policy (dead-letter queue)'. At the bottom right is a yellow 'Create subscription' button.

The screenshot shows the 'Subscription Details' page for a subscription with ARN 'arn:aws:sns:us-east-1:648045618926:MoneyAlert:330ddd50-1203-4b4d-ac1d-69b45f001b03'. The 'Status' is 'Confirmed'. The 'Protocol' is 'SMS'. The 'Topic' is 'MoneyAlert'. The 'Subscription Principal' is 'arn:aws:iam::648045618926:role/voclabs'. There are tabs for 'Subscription filter policy' and 'Redrive policy (dead-letter queue)'. At the bottom right are 'Edit' and 'Delete' buttons.

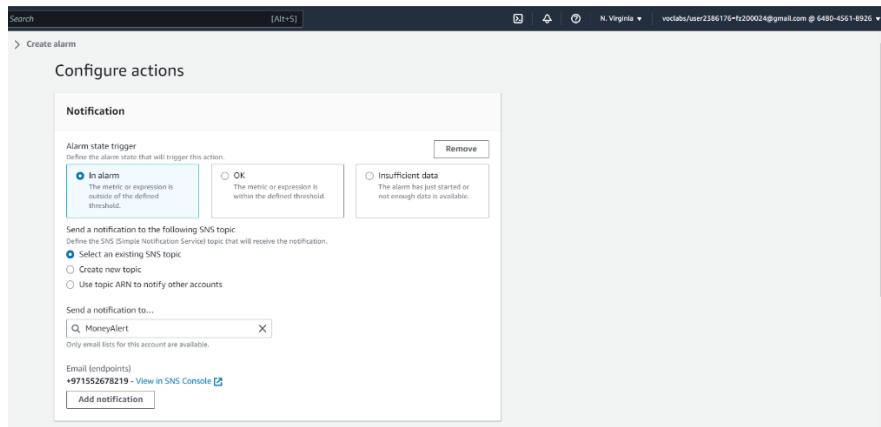
After this, a CloudWatch alarm is created. Since the alarm should monitor the estimated charge for EC2 only, therefore when selecting a metric, and then going to Billing>>By Services, The AmazonEC2 metric is selected.



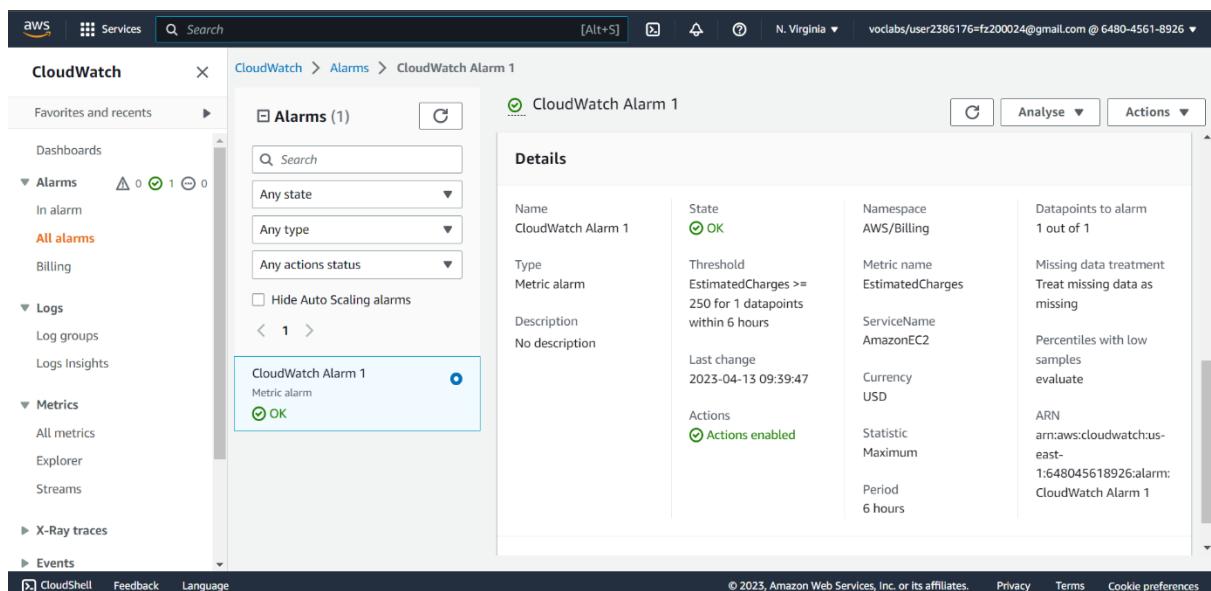
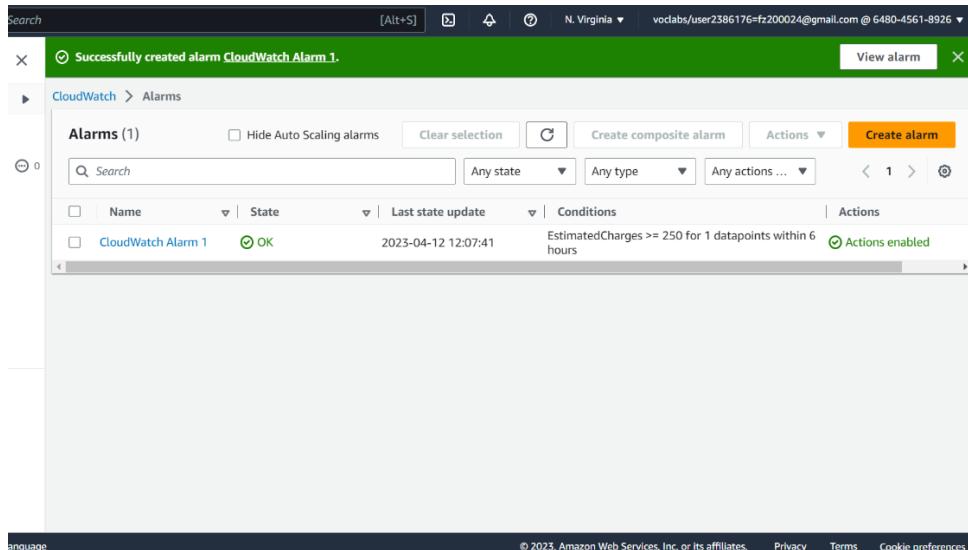
The alarm is then configured with a static threshold type, and the threshold value is defined as greater/equal to 250 USD.



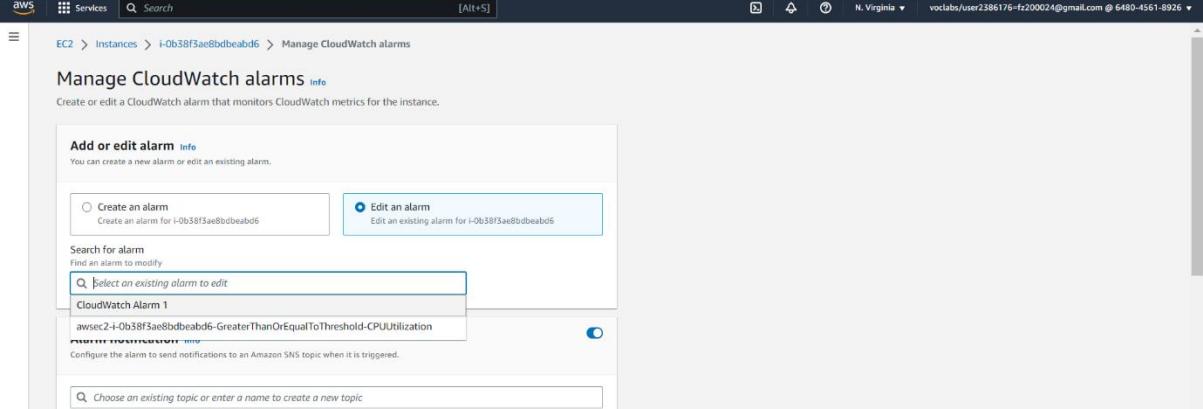
The alarm is meant to be created for the existing SNS topic of MoneyAlert.



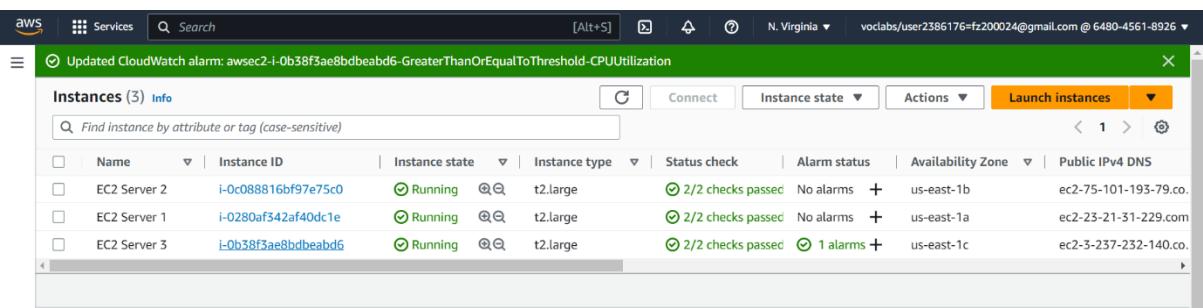
After finally configuring the alarm name as CloudWatch Alarm 1, the following is shown for cloud watch alarm:



This alarm is now to be attached to the EC2 Server 3 instance. This is done by adding an alarm to the EC2 Server 3 instance.



The screenshot shows the 'Manage CloudWatch alarms' interface. A radio button for 'Edit an alarm' is selected, with the text 'Edit an existing alarm for i-0b38f3ae8bdbeabd6'. Below it is a search bar labeled 'Select an existing alarm to edit' containing 'CloudWatch Alarm 1'. A dropdown menu lists 'awssec2-i-0b38f3ae8bdbeabd6-GreaterThanOrEqualToThreshold-CPUUtilization'. At the bottom, there's a note about configuring notifications to an Amazon SNS topic.



The screenshot shows the 'Instances (3) Info' page. It lists three instances: EC2 Server 2, EC2 Server 1, and EC2 Server 3, all in the 'Running' state. The table includes columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4 DNS. The 'Alarm status' column for EC2 Server 3 indicates '1 alarms'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
EC2 Server 2	i-0c088816bf97e75c0	Running	t2.large	2/2 checks passed	No alarms	us-east-1b	ec2-75-101-193-79.co.
EC2 Server 1	i-0280af342af40dc1e	Running	t2.large	2/2 checks passed	No alarms	us-east-1a	ec2-23-21-31-229.com
EC2 Server 3	i-0b38f3ae8bdbeabd6	Running	t2.large	2/2 checks passed	1 alarms	us-east-1c	ec2-3-237-232-140.co.

The three server load balance system creation is complete.

PART B:

To begin the creation of an S3 bucket with company specific data, an S3 bucket is created first with the name **companybuckets3**, and granted public access.

The screenshot shows the 'Create bucket' wizard in the AWS S3 console. In the 'General configuration' step, the bucket name is set to 'companybuckets3' and the AWS Region is set to 'US East (N. Virginia) us-east-1'. A note about copy settings from existing buckets is present. In the 'Block Public Access settings for this bucket' step, the 'Block all public access' checkbox is checked. A warning message states that turning off block all public access might result in the bucket becoming public. A checkbox for acknowledging this risk is checked. The 'Block all public access' checkbox is checked.

The screenshot shows the 'Buckets' page in the AWS S3 console. The sidebar includes options like 'Access Points', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', 'IAM Access Analyzer for S3', 'Block Public Access settings for this account', 'Storage Lens', 'Dashboards', 'AWS Organizations settings', and 'Feature spotlight'. The main area displays an 'Account snapshot' with total storage of 5.0 MB, object count of 1, and average object size of 5.0 MB. It also shows a table of buckets, with one entry for 'companybuckets3' which was created on April 12, 2023, at 05:23:32 UTC+04:00, located in the US East (N. Virginia) region, with public access.

The bucket permissions are then accessed, and modified by entering the following JSON code in the bucket policy text field to provide public access to the objects stored in the bucket.

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](#)

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "PublicReadGetObject",  
      "Effect": "Allow",  
      "Principal": "*",  
      "Action": "s3:GetObject",  
      "Resource": "arn:aws:s3:::companybuckets3/*"  
    }  
  ]  
}
```

[Copy](#)

After this, files and folders are uploaded to the bucket. The relevant files and folders of the company website are uploaded to the S3 bucket with the Standard storage class.

The screenshot shows the AWS Management Console with the Services navigation bar selected. The main content area is titled 'Storage class' and displays a table comparing different storage classes based on their design, availability, and cost characteristics.

Storage class	Designed for	Availability Zones	Min storage duration	Cost
Standard	Frequently accessed data (more than once a month) with milliseconds access	≥ 3	-	-
Intelligent-Tiering	Data with changing or unknown access patterns	≥ 3	-	-
Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days	1
One Zone-IA	Recreatable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access	1	30 days	1
Glacier Instant Retrieval	Long-lived archive data accessed once a quarter with instant retrieval in milliseconds	≥ 3	90 days	1
Glacier Flexible Retrieval (formerly Glacier)	Long-lived archive data accessed once a year with retrieval of minutes to hours	≥ 3	90 days	-

At the bottom of the interface, there are links for CloudShell, Feedback, Language, and cookie preferences, along with copyright information for Amazon Web Services, Inc. or its affiliates.

Then the salary log and the relevant files and folders of the media archives are uploaded to the S3 bucket with the Intelligent-Tiering storage class, since these objects consist of data with changing or unknown access patterns.

The screenshot shows the AWS Management Console with the search bar at the top. The URL in the address bar is `vocabs/user2386176=fz200024@gmail.com @ 6480-4561-8926`. The main content area is titled "Storage class" and contains a table comparing different storage classes based on their design, availability zones, and minimum storage duration. The "Intelligent-Tiering" class is highlighted with a blue border, indicating it is selected.

Storage class	Designed for	Availability Zones	Min storage duration
Standard	Frequently accessed data (more than once a month) with milliseconds access	≥ 3	-
Intelligent-Tiering	Data with changing or unknown access patterns	≥ 3	-
Standard-IA	Infrequently accessed data (once a month) with milliseconds access	≥ 3	30 days
One Zone-IA	Recreatable, infrequently accessed data (once a month) stored in a single Availability Zone with milliseconds access	1	30 days
Glacier Instant Retrieval	Long-lived archive data accessed once a quarter with instant retrieval in milliseconds	≥ 3	90 days
Glacier Flexible Retrieval (formerly Glacier)	Long-lived archive data accessed once a year with retrieval of minutes to hours	≥ 3	90 days

The S3 bucket files are then made to be publicly accessible via a CDN. A CloudFront Distribution is created for this purpose using the S3 bucket origin domain.

The screenshot shows the AWS Management Console with the search bar at the top. The URL in the address bar is `vocabs/user2386176=fz200024@gmail.com @ 6480-4561-8926`. The main content area is titled "Create distribution" and shows the "Origin" configuration section. An S3 bucket named "companybuckets3.s3.us-east-1.amazonaws.com" is selected as the origin. A warning message states that the S3 bucket has static web hosting enabled and recommends using the S3 website endpoint instead of the bucket endpoint. The "Name" field is populated with the same bucket name. The "Origin access" section is set to "Public".

Going to the companybuckets3 properties tab, the static website hosting settings are edited to be enabled for the bucket hosting type, and the index document is specified as index.html, which is the home page of the website.

Static website hosting
Use this bucket to host a website or redirect requests. [Learn more](#)

Static website hosting
 Disable
 Enable

Hosting type
 Host a static website
Use the bucket endpoint as the web address. [Learn more](#)
 Redirect requests for an object
Redirect requests to another bucket or domain. [Learn more](#)

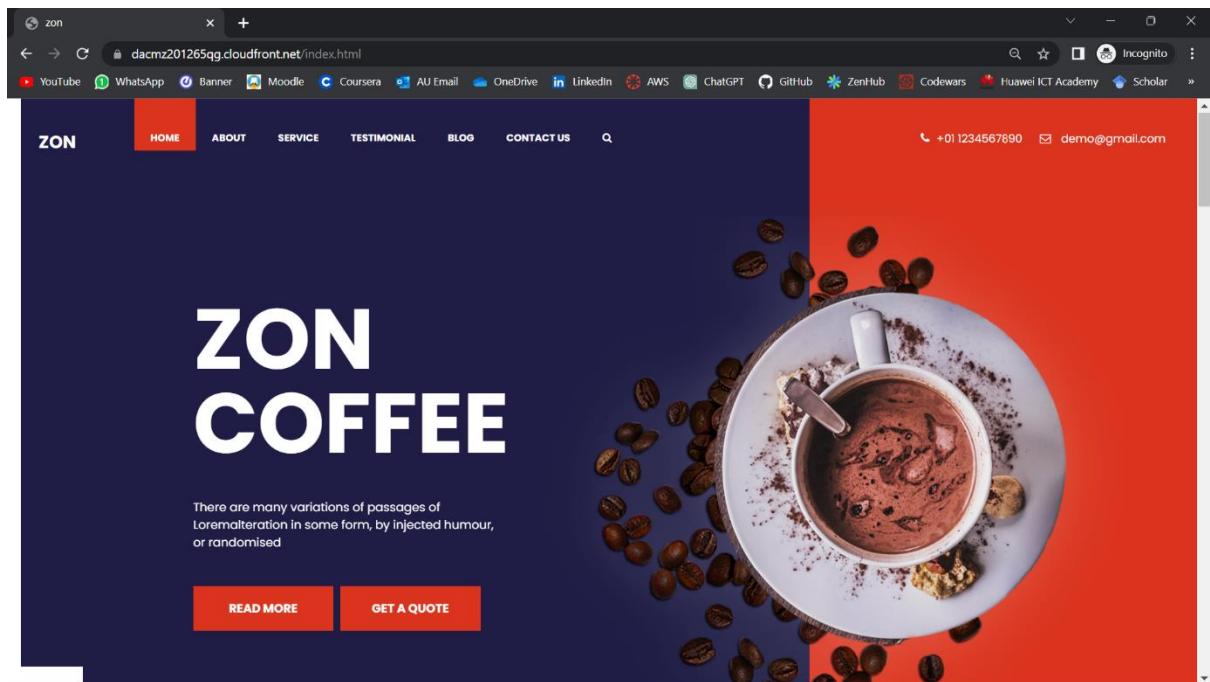
Index document
Specify the home or default page of the website.

From the recently created CloudFront distribution, the distribution domain name is copied and pasted into the search bar of the browser, and the path index.html is appended to it as it is the homepage of the website also specified while modifying the static web hosting setting in the S3 bucket, making the link look like:

<https://dacmz201265gq.cloudfront.net/index.html>

General	Origins	Behaviors	Error pages	Geographic restrictions	Invalidations	Tags
Details						
Distribution domain name dacmz201265gq.cloudfront.net	ARN arn:aws:cloudfront:648045618926:distribution/EPVNVK2POT3EG	Last modified April 12, 2023 at 5:49:13 AM UTC				
Settings						
Description -	Alternate domain names -	Standard logging Off				
Price class Use all edge locations (best performance)		Cookie logging Off				
Supported HTTP versions HTTP/2, HTTP/1.1, HTTP/1.0		Default root object -				
AWS WAF -						

This link makes the website in the company's S3 bucket publicly accessible via CDN.



The creation S3 bucket for company data is complete.

The cloud architecture has successfully been implemented according to the requirements given.