

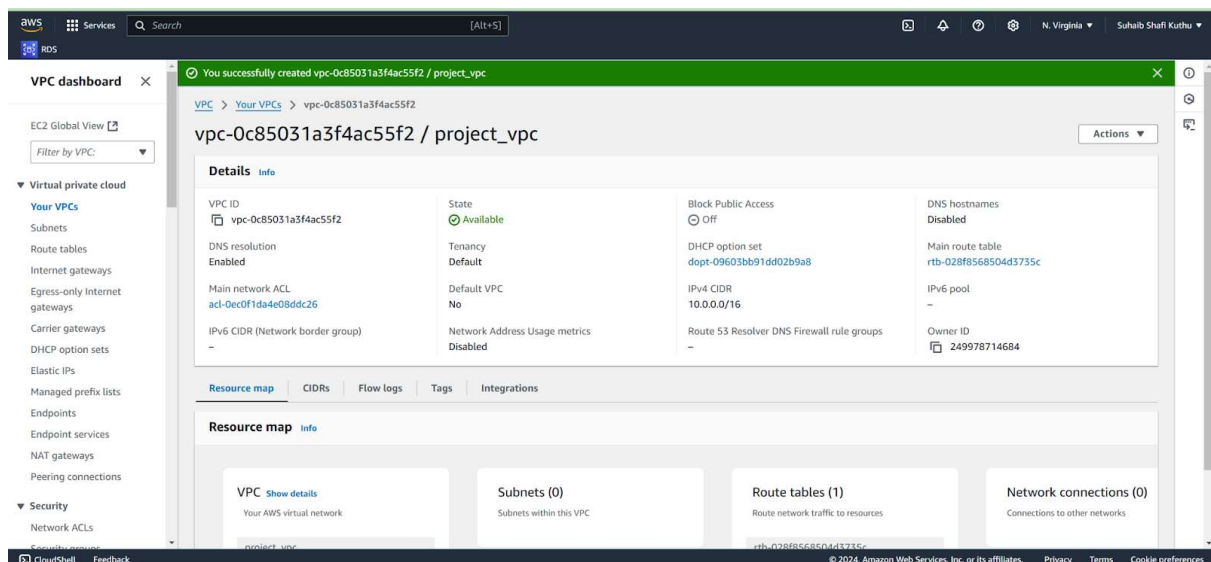
Project2

Below are the steps for the procedure to be followed to achieve the required architecture

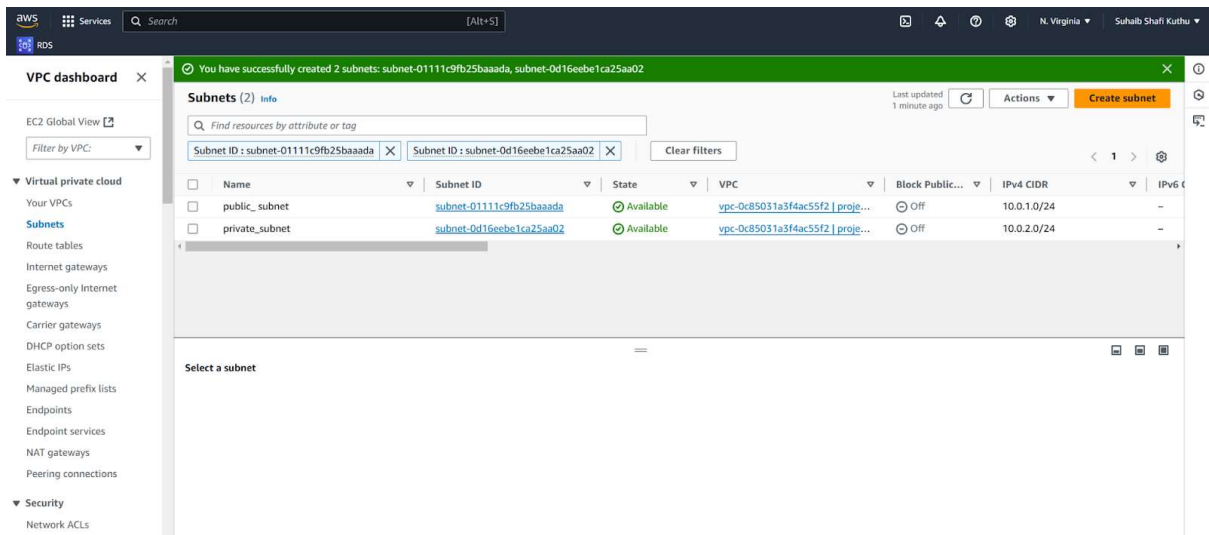
They are concerned about the security of the environment, so they have decided to virtually isolate their network from the rest of the customers and the rest of the environments in the same AWS Cloud Account

Step1:-

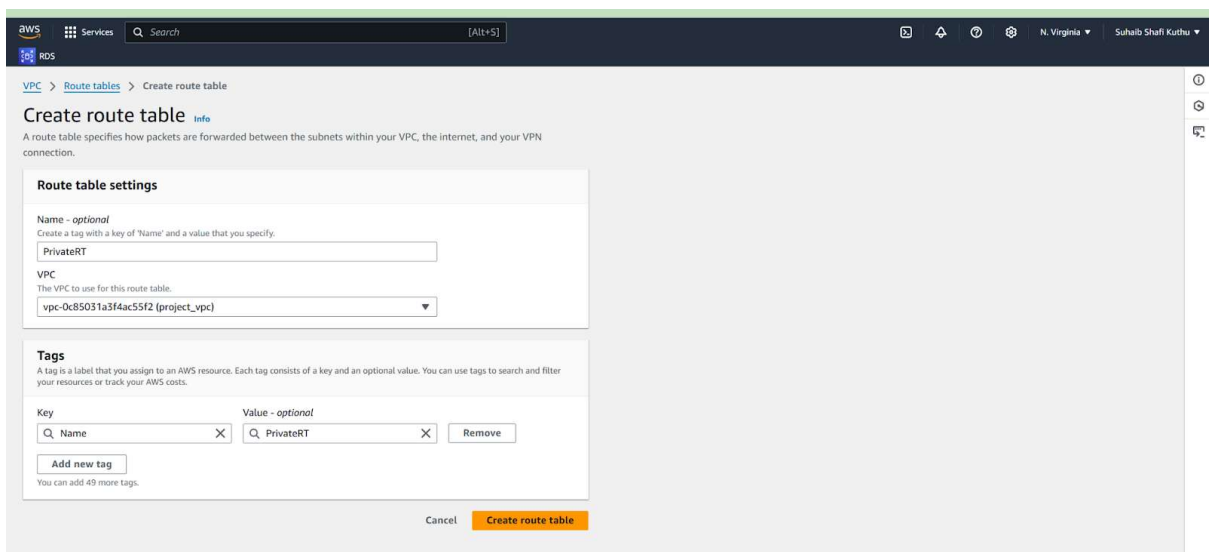
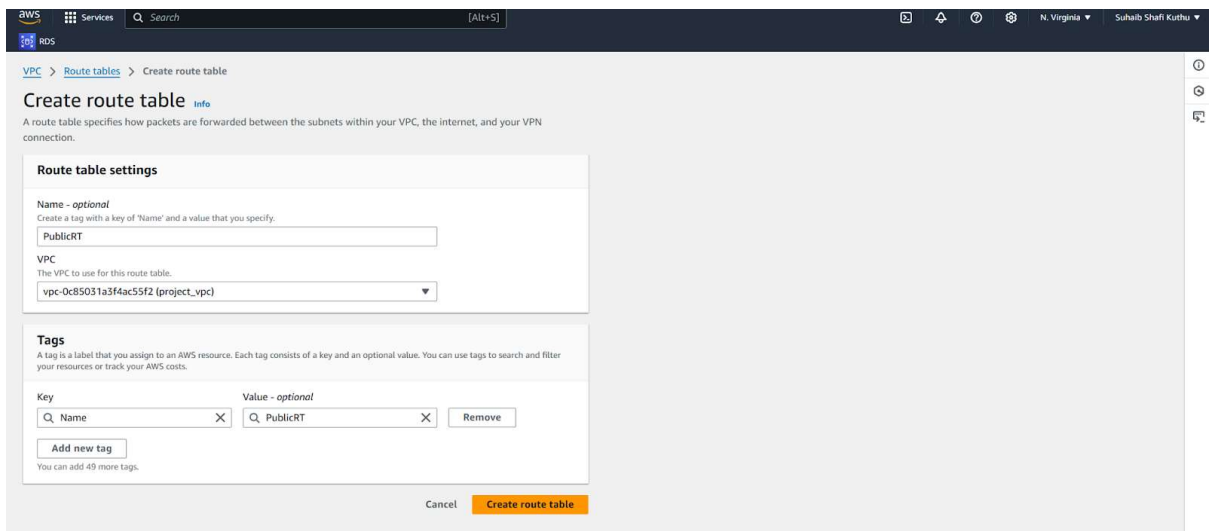
Create a vpc where the front end is kept in the public subnet and backend in private subnet.



Step 2:- create subnets in the vpc with public access and private access



Step 3 :- create route tables for public and private subnets and associate accordingly



Step 4

Subnet associations ,assoociate public subnet with publicRt and private subnet for public rt

VPC > Route tables > rtb-095c6b03b0ed5d4ed > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Filter subnet associations

<input checked="" type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	public_subnet	subnet-01111c9fb25baaada	10.0.1.0/24	-	Main (rtb-028f8568504d3735c)
<input type="checkbox"/>	private_subnet	subnet-0d16eebe1ca25aa02	10.0.2.0/24	-	Main (rtb-028f8568504d3735c)

Selected subnets

subnet-01111c9fb25baaada / public_subnet X

Cancel Save associations

VPC > Route tables > rtb-09c4bf2287fbbf1de > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (1/2)

Filter subnet associations

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/>	public_subnet	subnet-01111c9fb25baaada	10.0.1.0/24	-	rtb-095c6b03b0ed5d4ed / PublicRT
<input checked="" type="checkbox"/>	private_subnet	subnet-0d16eebe1ca25aa02	10.0.2.0/24	-	Main (rtb-028f8568504d3735c)

Selected subnets

subnet-0d16eebe1ca25aa02 / private_subnet X

Cancel Save associations

Step 5

Create an internet gateway and attach it to vpc to make it available outside as public url.

VPC dashboard X

EC2 Global View [x]

Filter by VPC: [v]

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only Internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections

Security

The following internet gateway was created: igw-0e1608e6560dc566e - Project_IG. You can now attach to a VPC to enable the VPC to communicate with the internet. Attach to a VPC X

VPC > Internet gateways > igw-0e1608e6560dc566e

igw-0e1608e6560dc566e / Project_IG

Actions

Details Info

Internet gateway ID	State	VPC ID	Owner
igw-0e1608e6560dc566e	Detached	-	249978714684

Tags

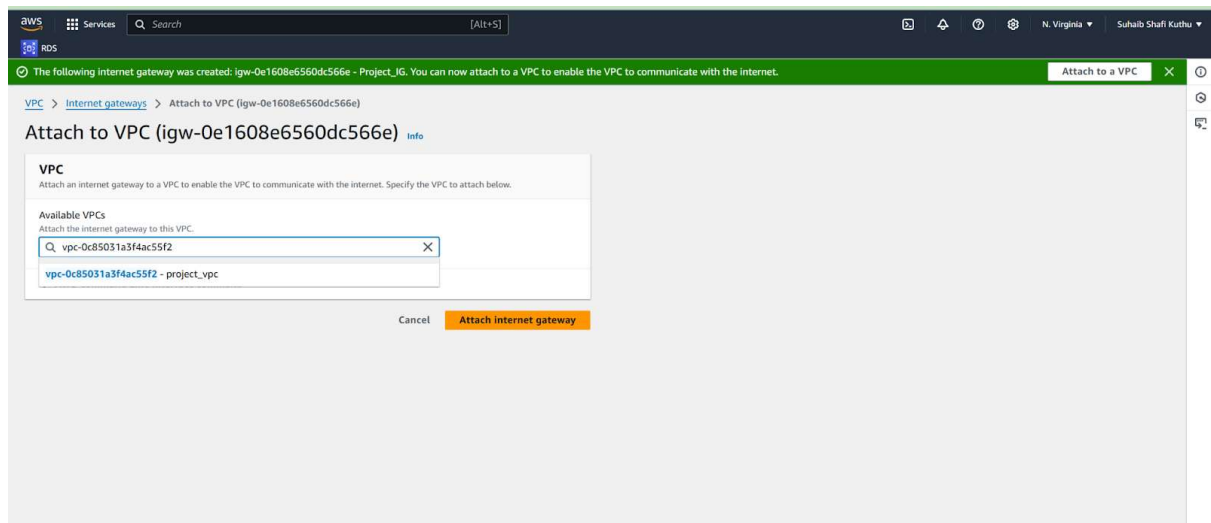
Search tags

Key	Value
Name	Project_IG

Manage tags

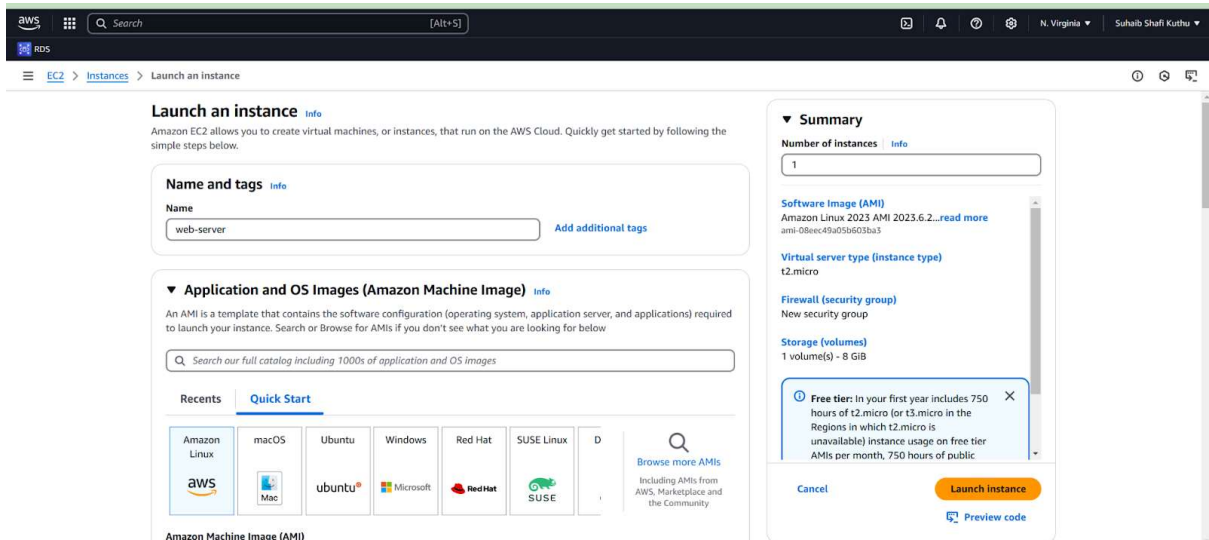
< 1 > [g]

Attach it created vpc



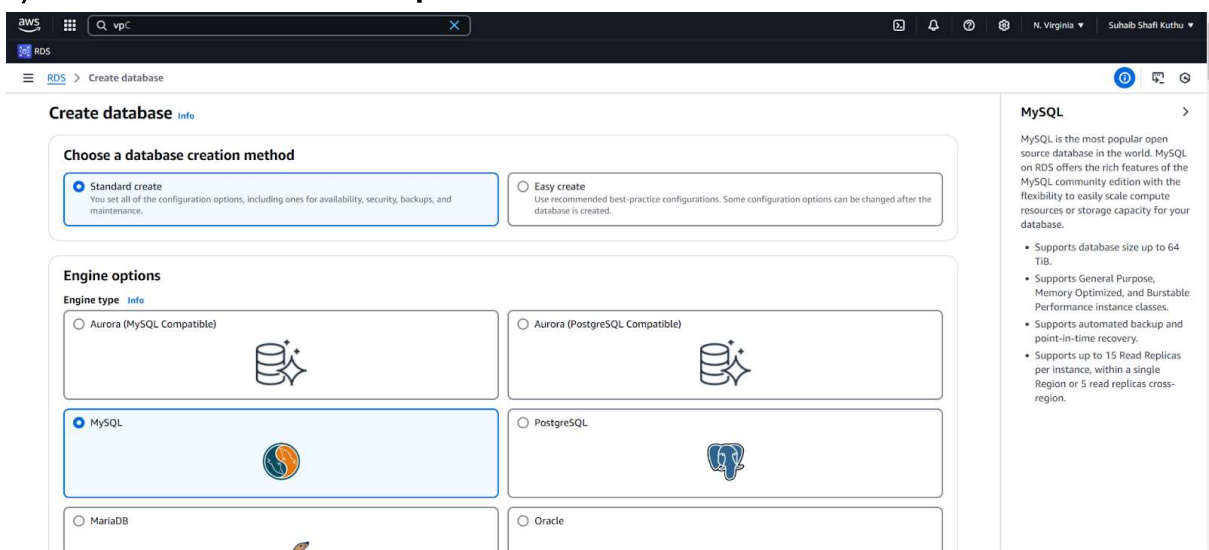
Due to the budget issue, the company cannot afford a dedicated DB engineer, So they are willing to outsource the DB management from a Cloud provider, to store and maintain the customer information received by PHP application. You must pick the right solution from AWS, which should be a Platform as a Service. It should also Provide high availability, patching, and back

Step 6 :- now go to the ec2 console and launch an instance to connect to database,the database and the server should be launched in the the same vpc that was created above.



As we need a platform as a service Db due to lack of dedicated db engineer, we can go with amazon RDS that could provide database solutions,as for the procedure follow the following steps.

- 1)Use Amazon RDS (MySQL or PostgreSQL) for a fully managed database solution.
- 2)Place the RDS instance in private subnets to enhance security.
- 3)Enable Multi-AZ Deployment for high availability.
- 4)Configure automatic backups, snapshots, and patching.
- 5)Create a DB Subnet Group to define which subnets RDS can use.



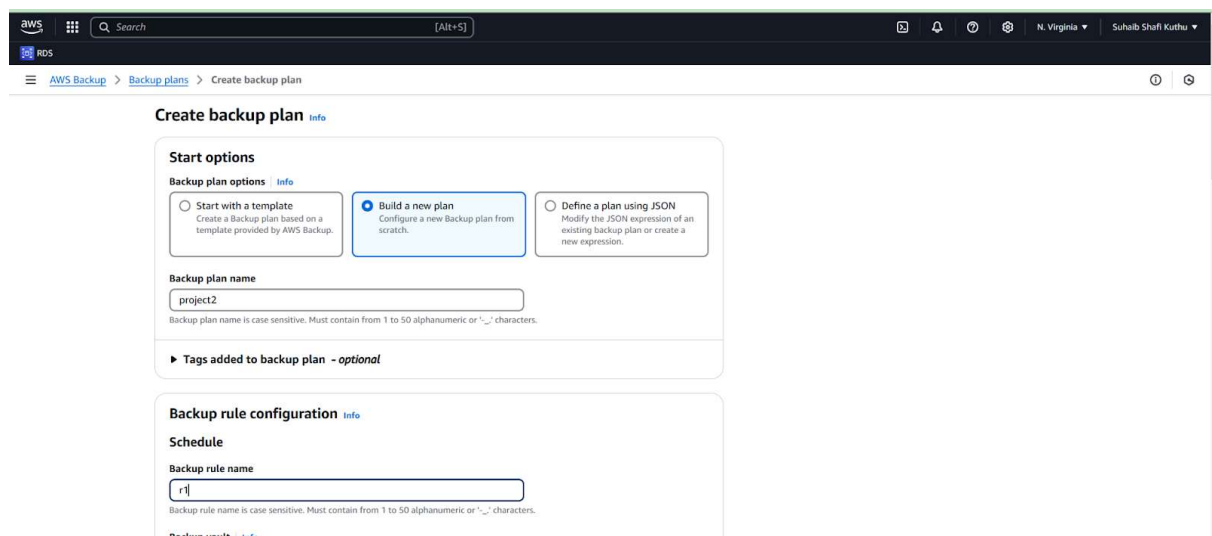
To retain the backup enable backups in database settings

Backups for your Web service may include creating snapshots of the instance or creating an Image of the Instance. Or

Enable AWS Backup for both EC2 and RDS instances.

Configure daily automated backups and retain snapshots based on the company's retention policy.

Use Cross-Region Replication to store critical backups in another region for additional resilience.

The screenshot shows the AWS Backup console interface for creating a new backup plan. The breadcrumb navigation at the top indicates the path: AWS Backup > Backup plans > Create backup plan. The main heading is 'Create backup plan' with an 'Info' link. Under the 'Start options' section, there are three radio buttons: 'Start with a template' (unselected), 'Build a new plan' (selected), and 'Define a plan using JSON' (unselected). Below these, the 'Backup plan name' field contains the text 'project2'. A note below the field states: 'Backup plan name is case sensitive. Must contain from 1 to 50 alphanumeric or "_" characters.' There is also a section for 'Tags added to backup plan - optional'. The 'Backup rule configuration' section is partially visible, showing a 'Schedule' subsection with a 'Backup rule name' field containing 'r1'. A note below this field states: 'Backup rule name is case sensitive. Must contain from 1 to 50 alphanumeric or "_" characters.'

Design a dynamic website where the customers can enter their details, which should be stored in a database, They are uncertain about the traffic pattern that how low or high it can be, so they have a requirement that the environment should be running at least two EC2 servers all time, and when there is a high load, they must burst up to four servers in total

Both of these could be achieved simultaneously

First go to the ec2 console and launch an ec2 instance,,to host the application download a web server in the instance

then create an ami of the instance ,and create a launch template out of that ami and use it in the creation of auto scaling group

aws [Search] [Alt+S] N. Virginia Suhail Shafi Kuthu

EC2 > Auto Scaling groups > Create Auto Scaling group

Choose instance launch options

Step 3 - optional: Integrate with other services

Step 4 - optional: Configure group size and scaling

Step 5 - optional: Add notifications

Step 6 - optional: Add tags

Step 7: Review

Name

Auto Scaling group name

Enter a name to identify the group.

Projectgrp

Must be unique to this account in the current Region and no more than 255 characters.

Launch template [Info](#)

For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Launch template

Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

temp1

[Create a launch template](#)

Version

Default (1)

[Create a launch template version](#)

Description

v1

Launch template

temp1 [Info](#)

It-09665cf4f1ea774a2

Instance type

t2.micro

AMI ID

Security groups

Request Spot Instances

In the further steps choose the availability zones in which the instances should be launched for high availability

aws [Search] [Alt+S] N. Virginia Suhail Shafi Kuthu

EC2 > Auto Scaling groups > Create Auto Scaling group

172.31.0.0/20 - Unavailable

[Create a VPC](#)

Availability Zones and subnets

Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets

us-east-1a | subnet-0fd7a86c81930bd43 | 172.31.80.0/20 | Default

us-east-1b | subnet-09eacd883aaf53606 | 172.31.16.0/20 | Default

us-east-1c | subnet-051db481569cd2c98 | 172.31.32.0/20 | Default

us-east-1d | subnet-07cf73343528110b9 | 172.31.0.0/20 | Default

[Create a subnet](#)

Availability Zone distribution - new

Auto Scaling automatically balances instances across Availability Zones. If launch failures occur in a zone, select a strategy.

☒ **Balanced best effort**

If launches fail in one Availability Zone, Auto Scaling will attempt to launch in another healthy Availability Zone.

☐ **Balanced only**

If launches fail in one Availability Zone, Auto Scaling will continue to attempt to launch in the unhealthy Availability Zone to preserve balanced distribution.

[Cancel](#) [Skip to review](#) [Previous](#) [Next](#)

The application should be highly available, even if a VM fails to respond to queries, there should be a mechanism to shift the connection to another healthy VM automatically

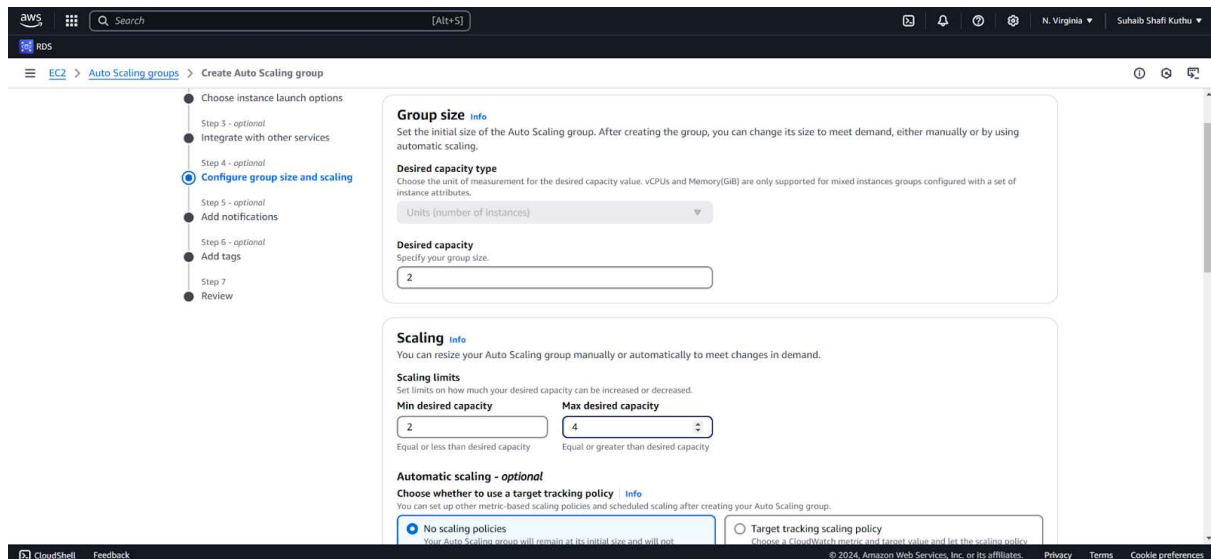
Here we will launch a load balancer within the auto-scaling group for load distribution

The screenshot shows the AWS Management Console interface for creating an Auto Scaling group. The breadcrumb navigation indicates the path: **EC2** > **Auto Scaling groups** > **Create Auto Scaling group**. A progress bar on the left lists the steps: Step 4 - optional (Configure group size and scaling), Step 5 - optional (Add notifications), Step 6 - optional (Add tags), Step 7 (Review), and the current step, Step 8 (Attach to a new load balancer). At the top, three radio buttons allow selecting the load balancer attachment: 'No load balancer', 'Attach to an existing load balancer', and 'Attach to a new load balancer' (which is selected). The 'Attach to a new load balancer' section contains the following fields: 'Load balancer type' with 'Application Load Balancer' selected; 'Load balancer name' with 'Projectgrp-1'; 'Load balancer scheme' with 'Internet-facing' selected; and 'Network mapping' with VPC 'vpc-001fe72604b821f76' selected. The footer of the console shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc.

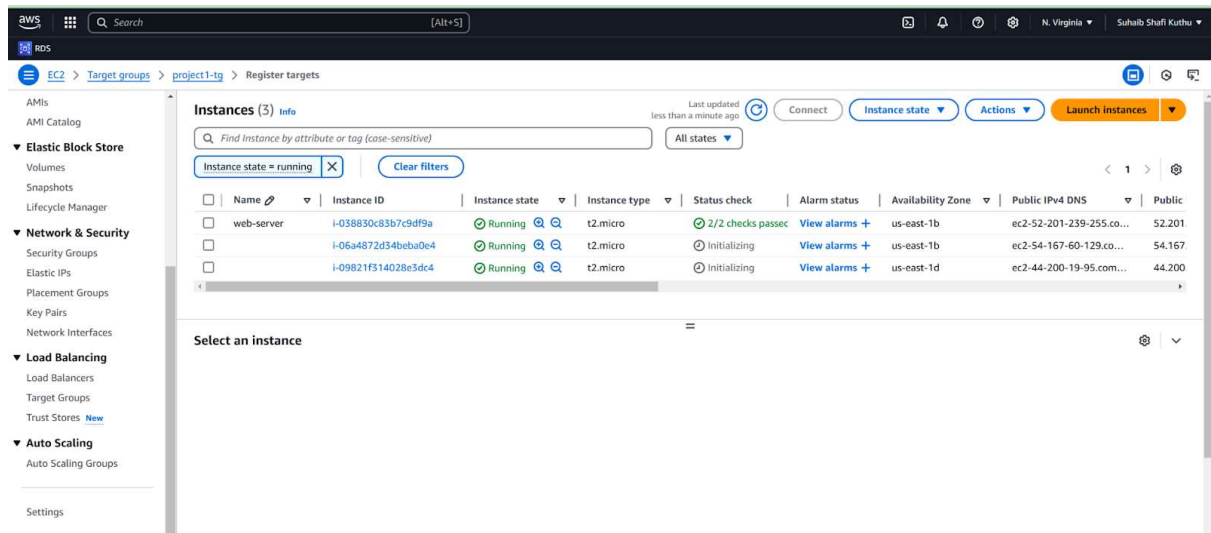
Also create a target group for load banner to distribute the traffic to

This screenshot shows the 'Listeners and routing' configuration page for a new load balancer. At the top, there is a 'Select a subnet' dropdown menu. The 'Listeners and routing' section includes a note about configuring listeners from the Load Balancing console. It features a 'Protocol' dropdown set to 'HTTP' and a 'Port' input field set to '80'. The 'Default routing (forward to)' section has a 'Create a target group' button and a 'New target group name' input field containing 'Projectgrp2'. Below this, the 'Tags - optional' section provides information about adding tags to the resource, with an 'Add tag' button and a note that 50 tags remain. At the bottom, the 'VPC Lattice integration options' section is visible, with an 'Info' link and a brief description of VPC Lattice integration.

Now in group size and scaling specify the minimum as maximum desired capacity as per the project it is 2 and 4



Go Ahead and launch
As we can see two more instances have been launched by ASG



Now the company cannot afford a dedicated engineer for monitoring, so you must automate the incident management through an event notification. Anytime there is an increase and decrease in the VM's due to high or low traffic, you must receive a notification via email.

To achieve this step we can go to billing and alarms and create and alarm and in the select metric section choose cpu utilization

Now in specify metric and condition choose greater than 70%

aws [Alt+S]

RDS CloudWatch Alarms Create alarm

69 04:30 05:30 06:30 CPUUtilization

Statistic: Average

Period: 5 minutes

Conditions

Threshold type

☒ Static Use a value as a threshold

☐ Anomaly detection Use a band as a threshold

Whenever CPUUtilization is...
Define the alarm condition.

☒ Greater > threshold

☐ Greater/Equal >= threshold

☐ Lower/Equal <= threshold

☐ Lower < threshold

than...
Define the threshold value.

70

Must be a number

▶ Additional configuration

CloudShell Feedback © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Now in configure actions configure sns topic to send a notification for the same

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

Configure actions

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

☒ In alarm The metric or expression is outside of the defined threshold.

☐ OK The metric or expression is within the defined threshold.

☐ Insufficient data The alarm has just started or not enough data is available.

Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

☐ Select an existing SNS topic

☒ Create new topic

☐ Use topic ARN to notify other accounts

Create a new topic...
The topic name must be unique.

projecttopic

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

suhairshafikuthu@gmail.com

user1@example.com, user2@example.com

Create topic

Add name and description

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

Configure actions

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

☒ In alarm The metric or expression is outside of the defined threshold.

☐ OK The metric or expression is within the defined threshold.

☐ Insufficient data The alarm has just started or not enough data is available.

Send a notification to the following SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

☐ Select an existing SNS topic

☒ Create new topic

☐ Use topic ARN to notify other accounts

Create a new topic...
The topic name must be unique.

projecttopic

SNS topic names can contain only alphanumeric characters, hyphens (-) and underscores (_).

Email endpoints that will receive the notification...
Add a comma-separated list of email addresses. Each address will be added as a subscription to the topic above.

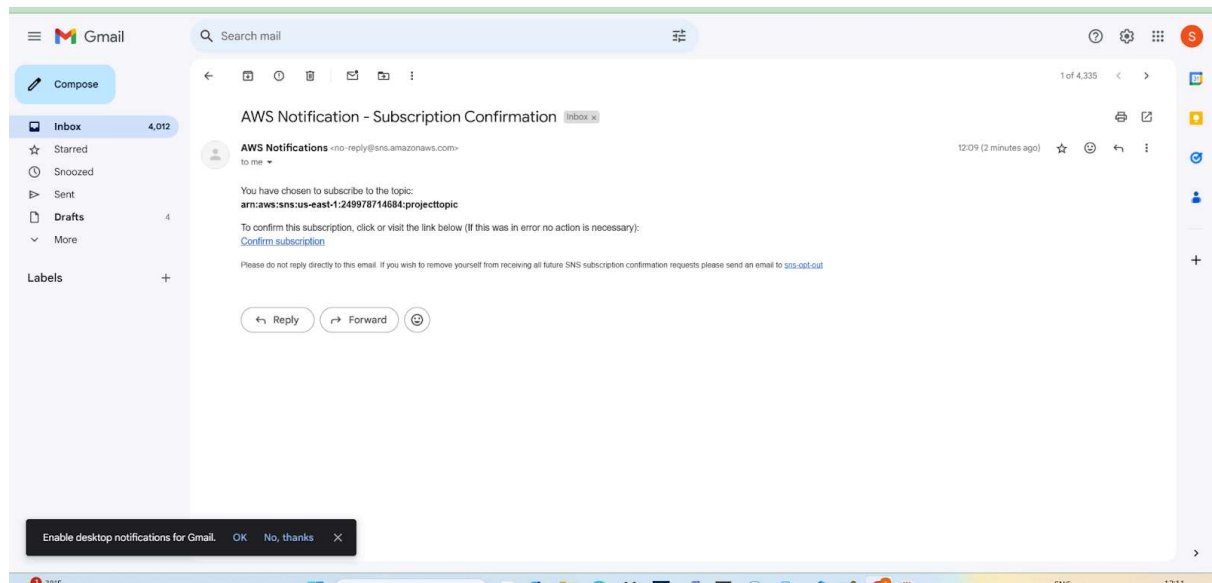
suhairshafikuthu@gmail.com

user1@example.com, user2@example.com

Create topic

Go on and create the alarm

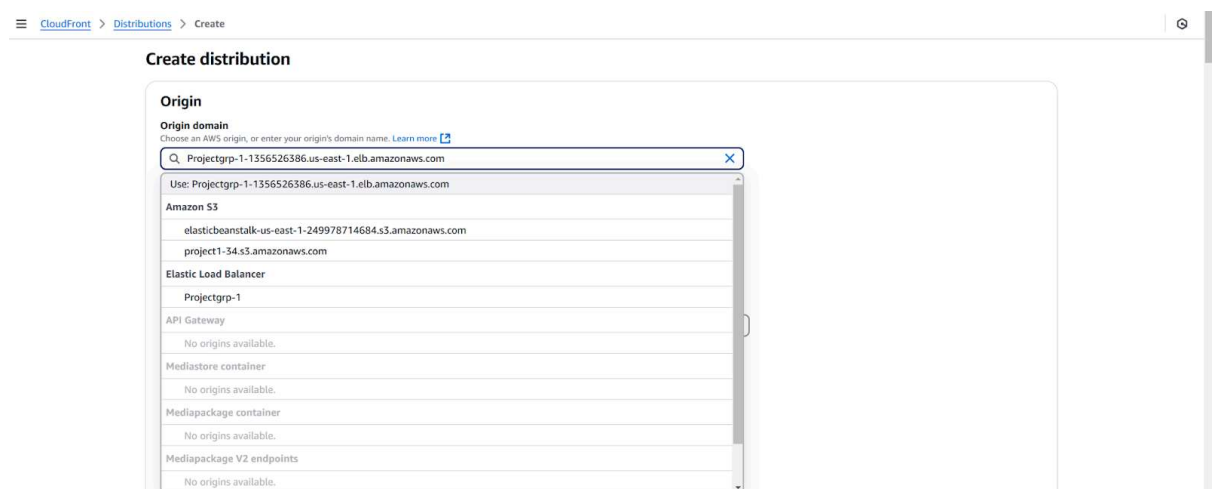
One more important thing dont forget to accept subscription which would be sent to registered e-mail Id



Your Dynamic Website should also be cached globally, so users worldwide can access it with less latency. The customer is okay if we get an unfriendly AWS generated URL for accessing the website

To achieve this follow

Create a CloudFront distribution to cache our application globally. Navigate to your CloudFront and click on create distribution Under web section click on get started On the Create Distribution page,under Origin Settings, choose the ELB that you created earlier Give the original path as project.php



Choose the origin domain the dns or the load balancer created above and keep the rest settings as default

Hence following the steps we can design a highly available php application with the need requirements.

