Project-ID-101-Three Tier Architecture(Expense note)

Objective:

A **highly available three-tier architecture** is to ensure scalability, fault tolerance, and seamless performance for user interactions. The **presentation tier** (Windows EC2 web server) collects user inputs (Integer & string). The **application tier** (running on the EC2 server) processes and stores data in an **RDS database**. The **database tier** (Amazon RDS) ensures reliable storage, This architecture eliminates single points of failure and can be enhanced with **auto-scaling and load balancing** for improved availability.

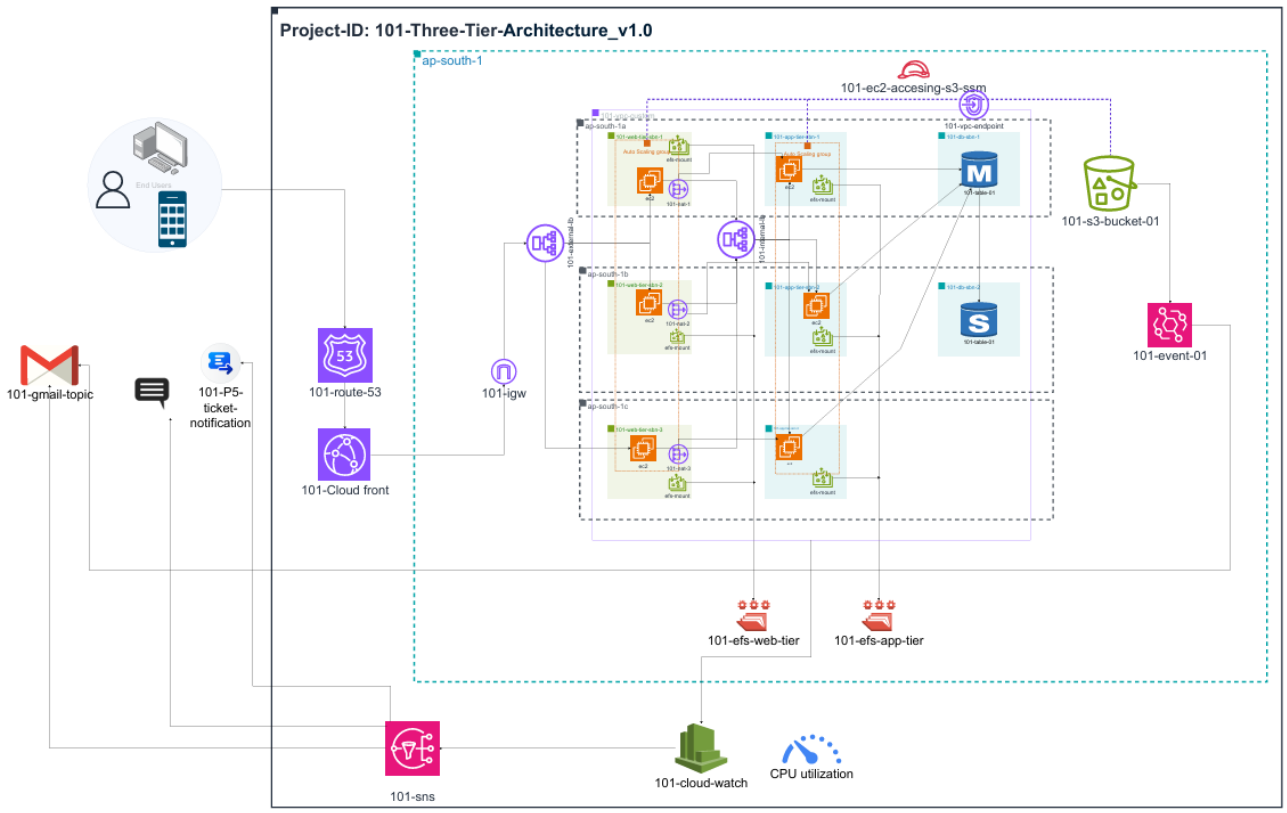
Architecture flow:

Route53 → Cloudfront →External Load balancer(Internet facing) → Auto scaling → Web tier → Internal Load balancer(Non Internet facing) → App tier → Database tier | VPC Endpoint(Gateway) | EFS |

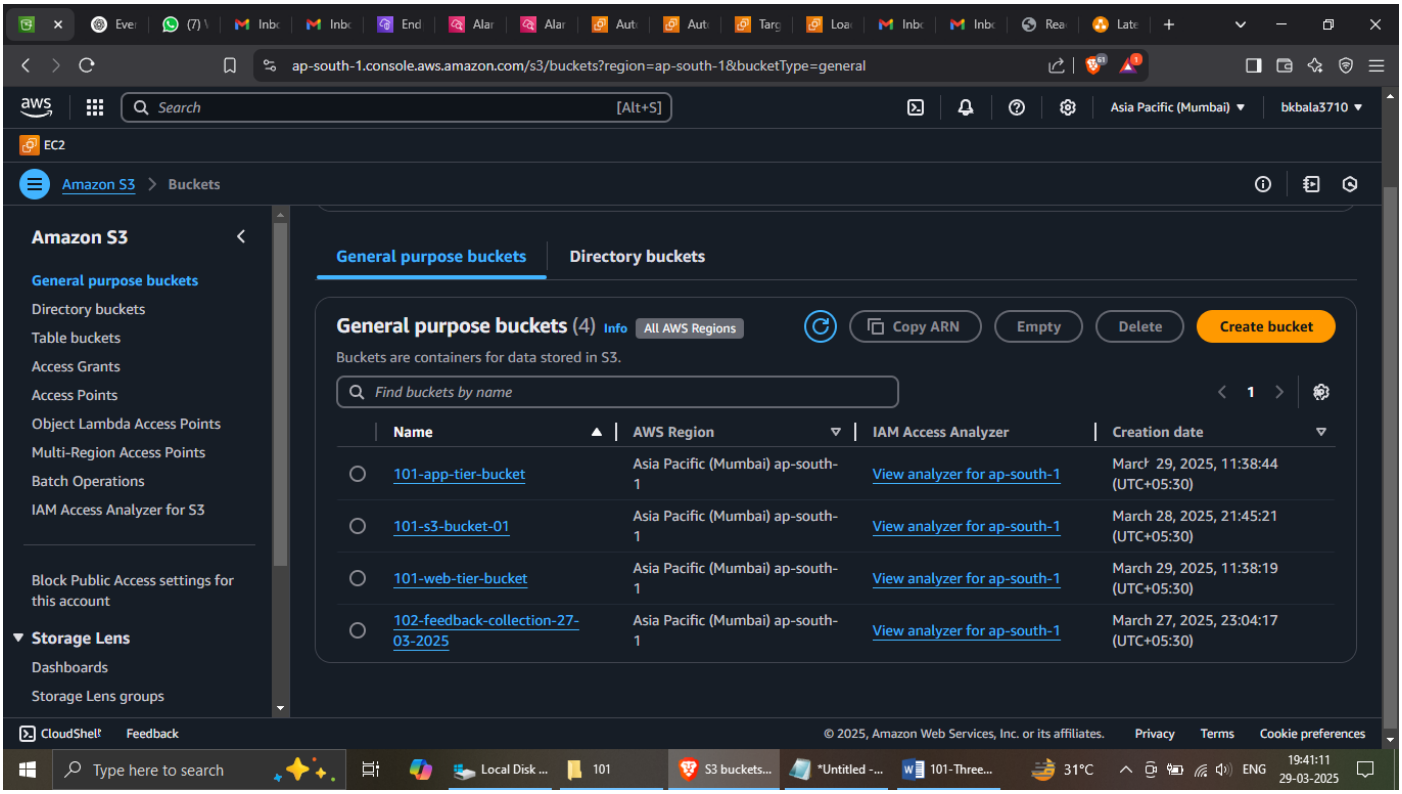
AWS Services required

1. Load balancer	7. NAT Gateway – Private subnet	12. VPC Endpoint
2. Autoscaling	8. SNS	13. EFS
3. EC2	9. Cloud Watch - Alarm	14. IAM
5. Security Group	10. S3	15. Route 53
6. Internet Gateway – Public subnet	11. AMI	16. Cloudfront

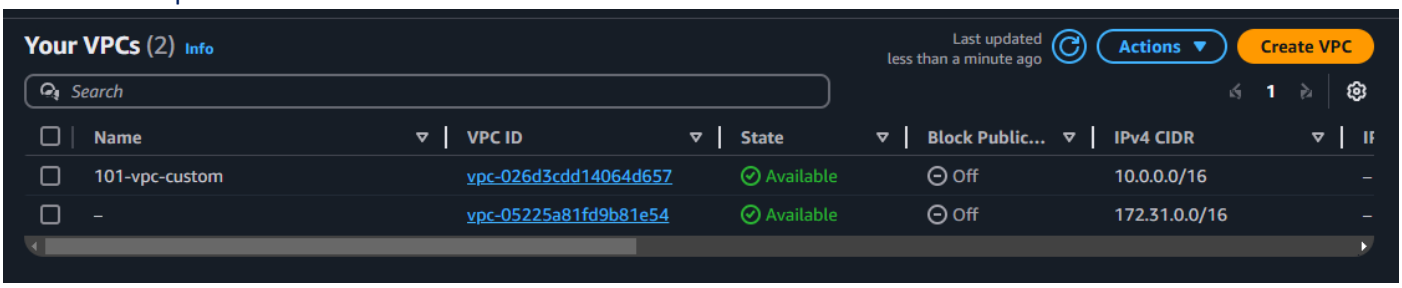
101-Three Tier Architecture(Expense note)_v1.0



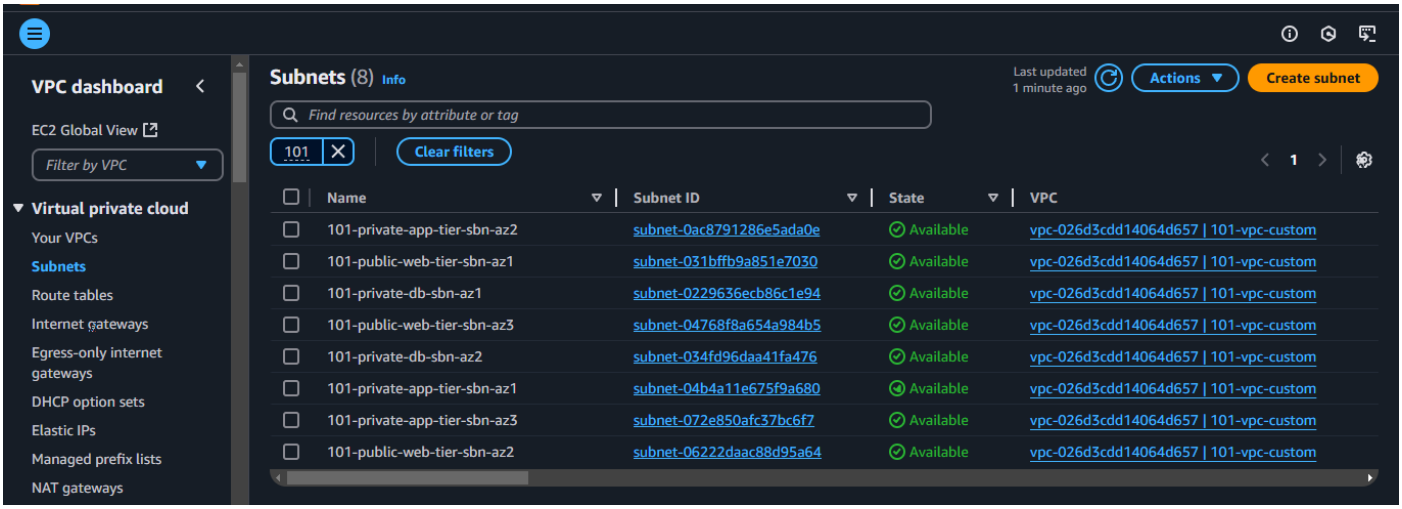
1. S3



2. VPC – 101-vpc-custom



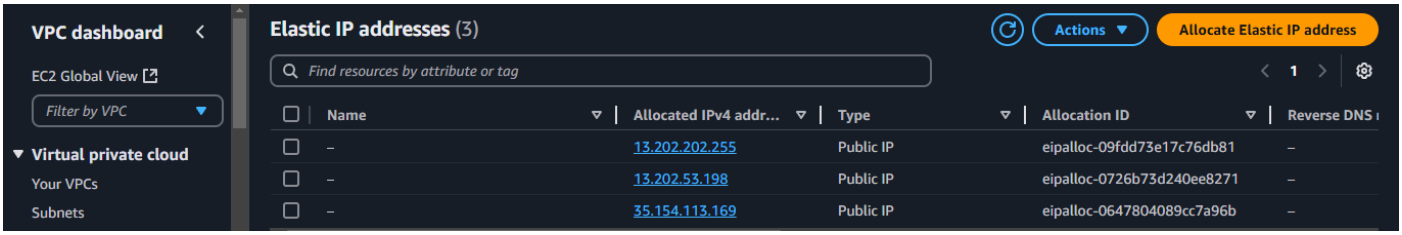
3. Subnet – 3(Public-Web-tier in 3az) | 3(Private-App-tier in 3az) | 2(Private - DB in 2az) = 8 Subnets



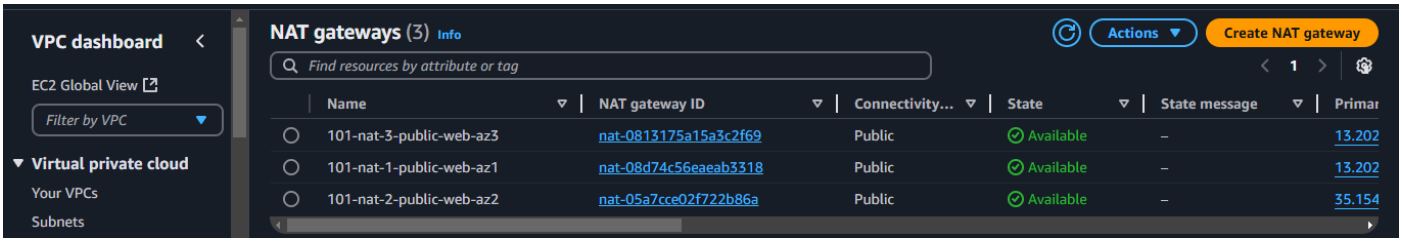
4. Route table – 1 Public (3az) | 3 Private for each NAT in each az(3az-private) | 1 private for db in 2az

5. IGW-vpc

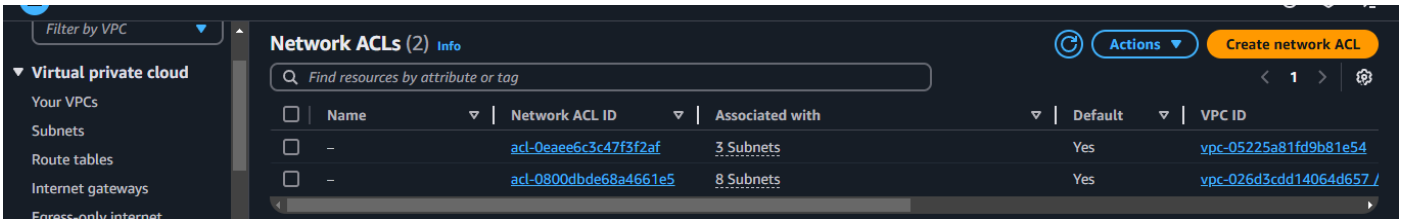
6. Elastic IP 3 for 3 NAT in 3az public to provide one way internet access to 3az private



7. 3NAT in 3az public

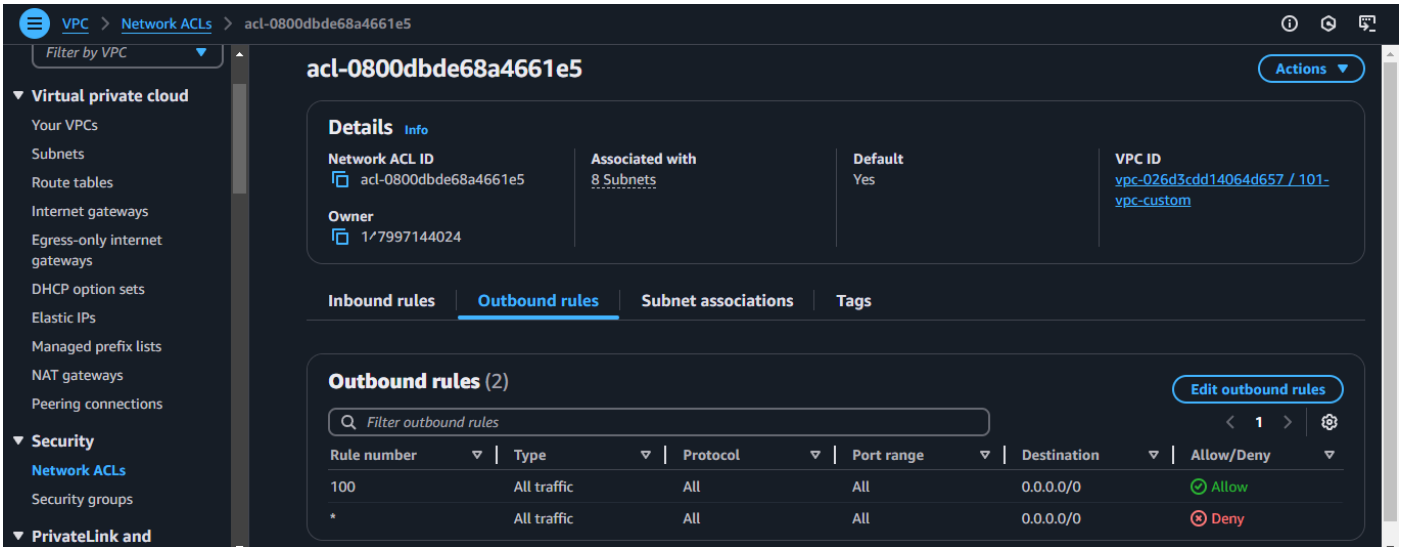


8. NACLs - 1 - VPC

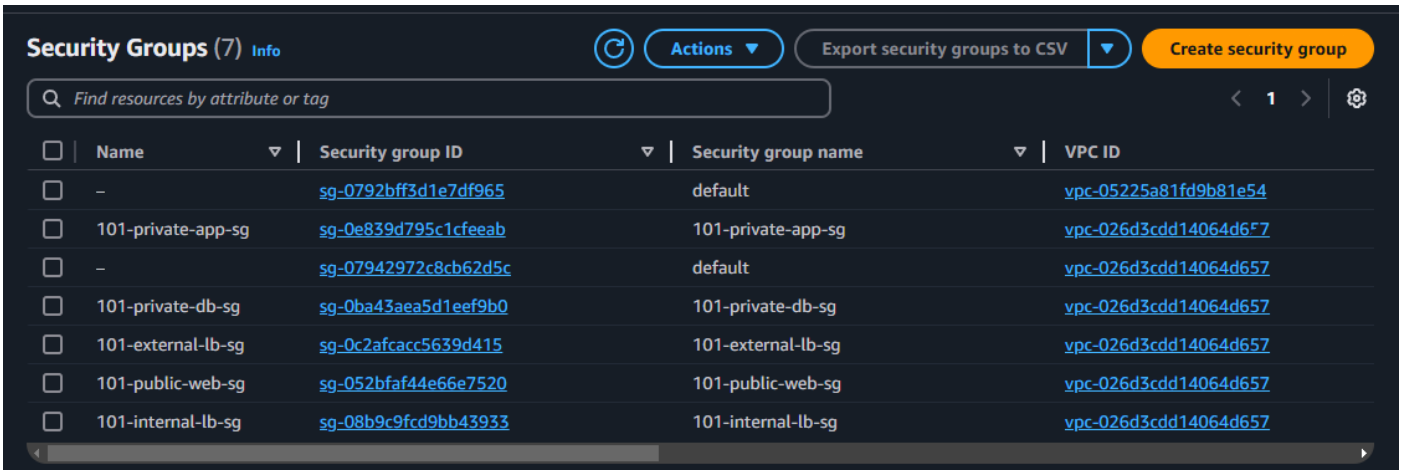


8.1. NACLS - inbound

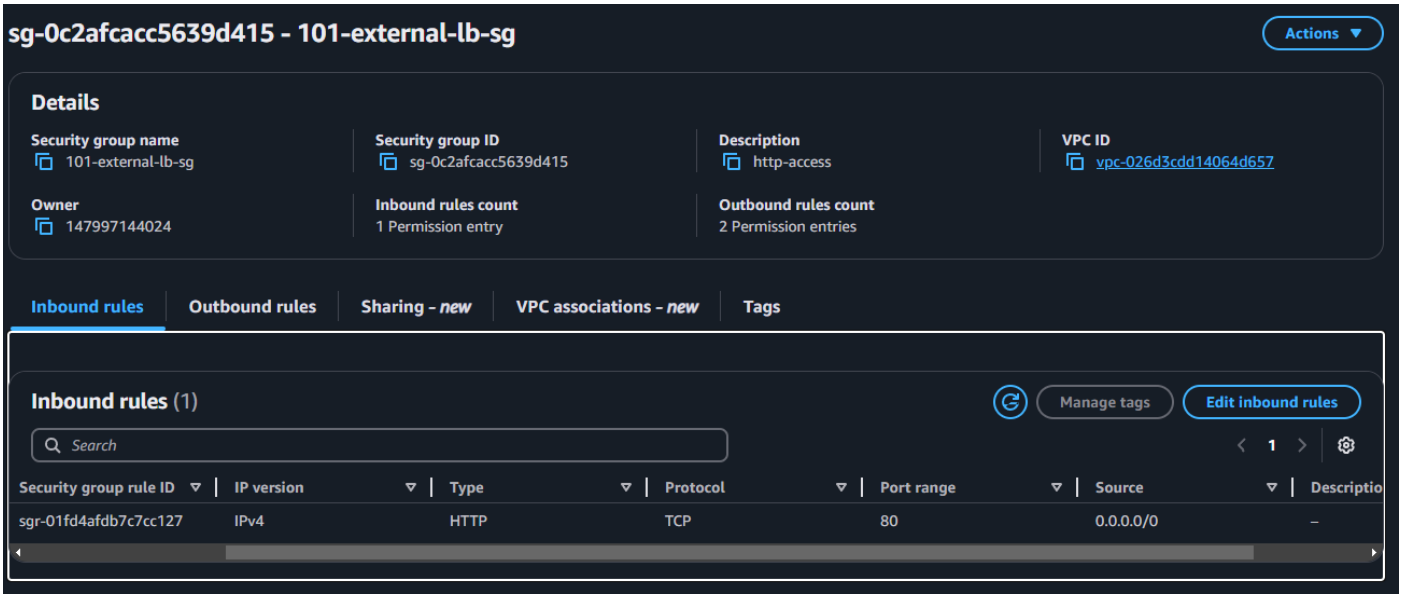
8.2. NACLs - Outbound



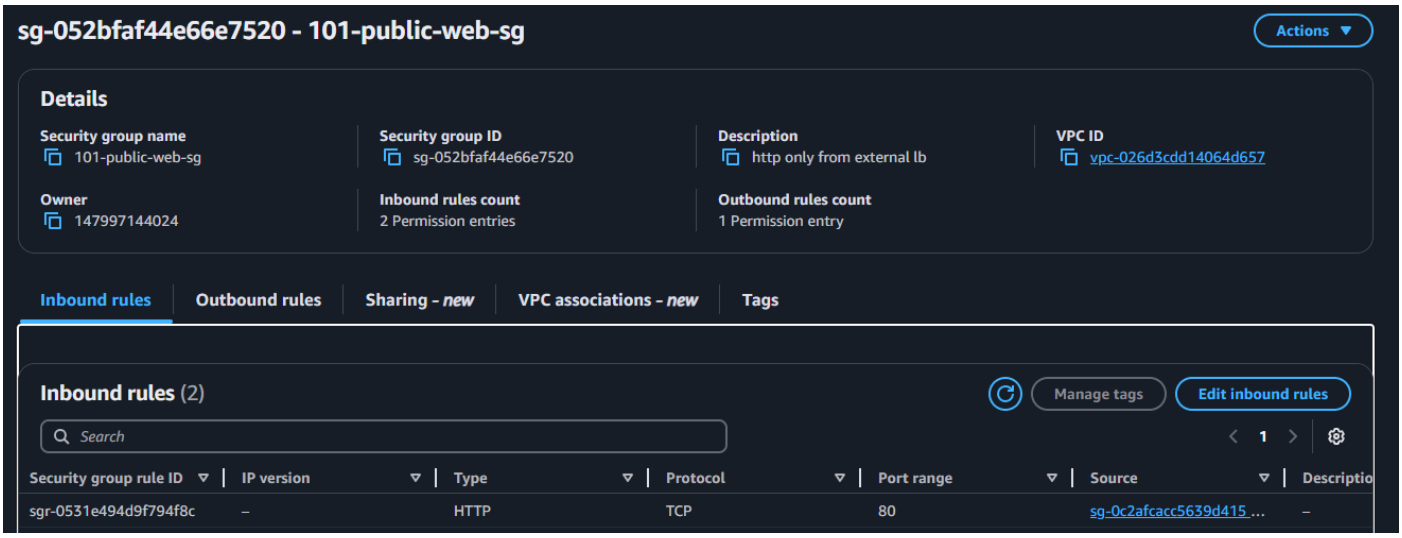
9. Security groups - 5



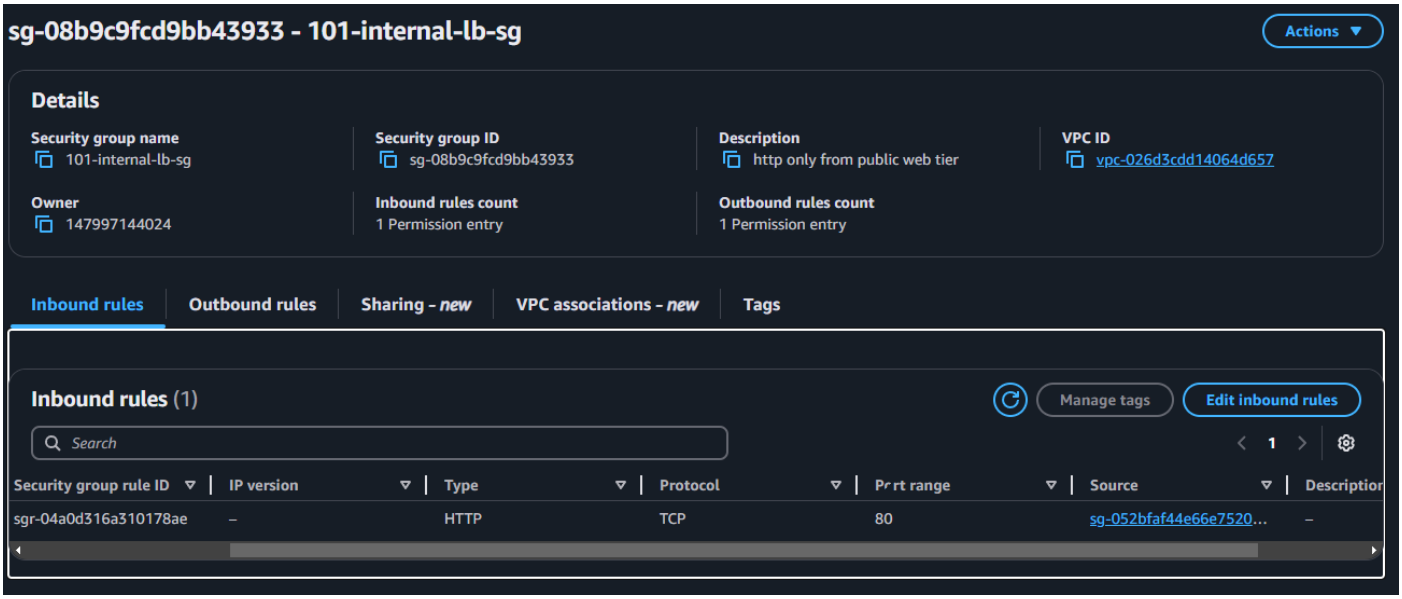
9.1. Security group of external load balancer allows only HTTP(80)



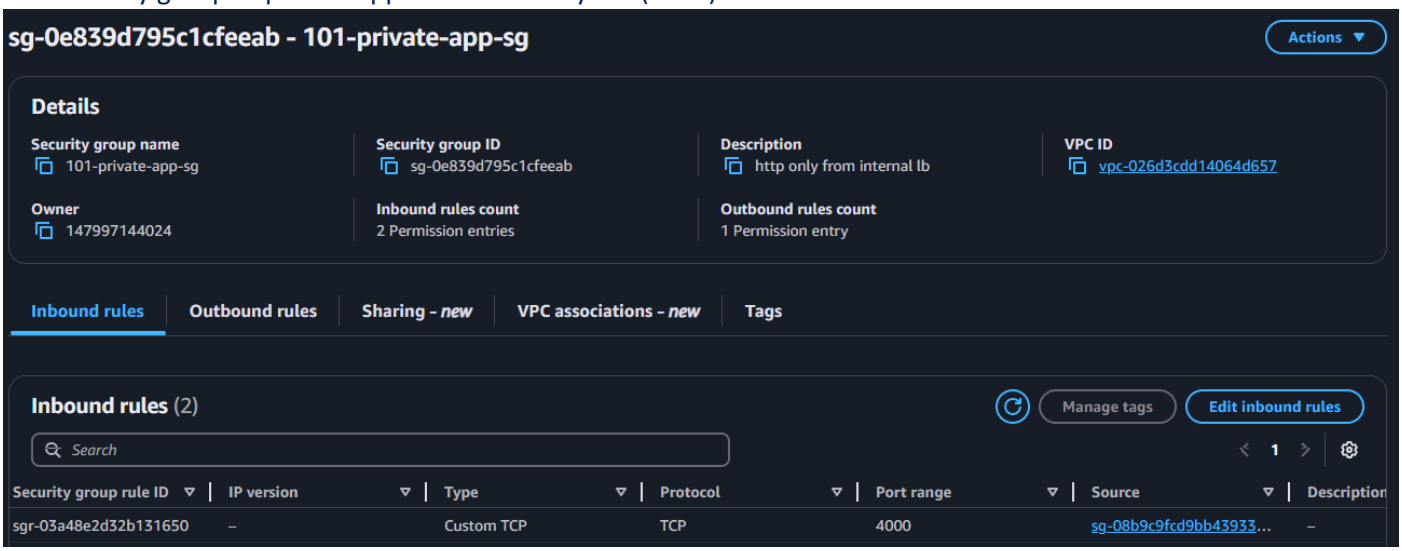
9.2. Security group of public web tier allows only HTTP(80) from external load balancer SG



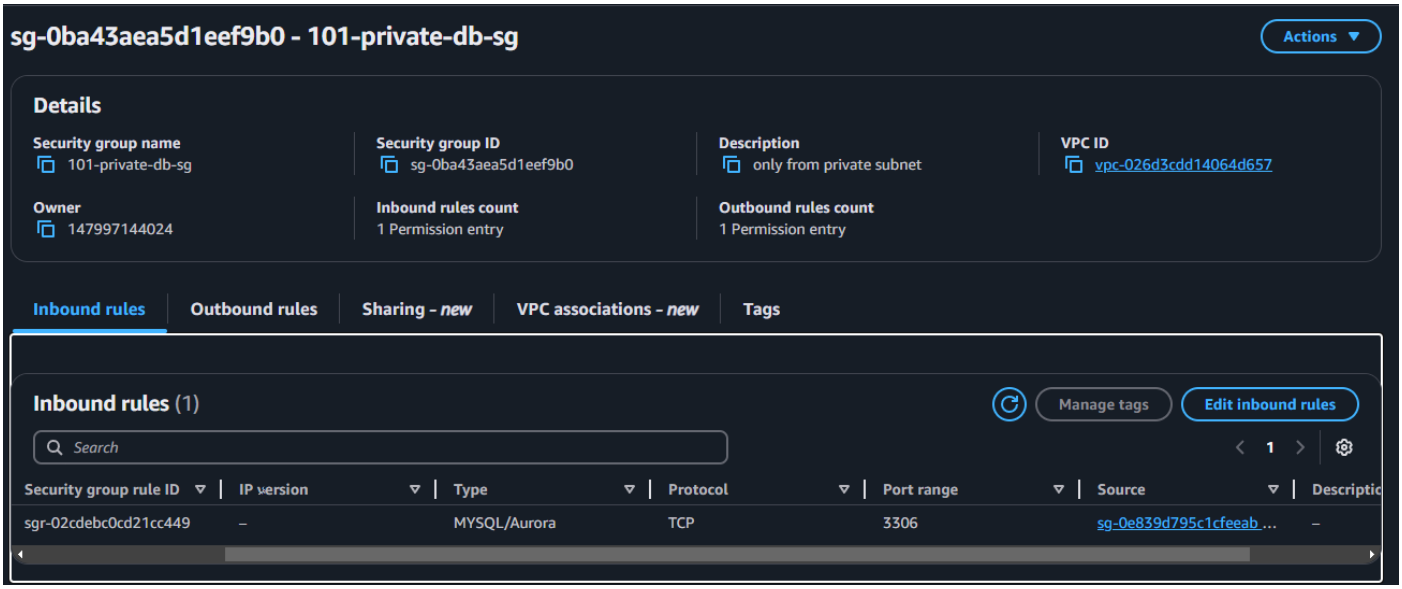
9.3. Security group of internal load balancer allows only HTTP(80) from web tier SG



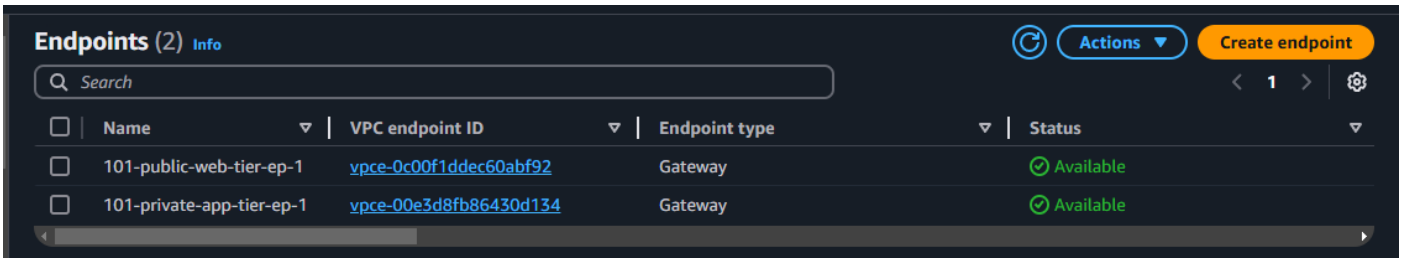
9.4. Security group of private app tier allows only TCP(4000) from internal load balancer SG



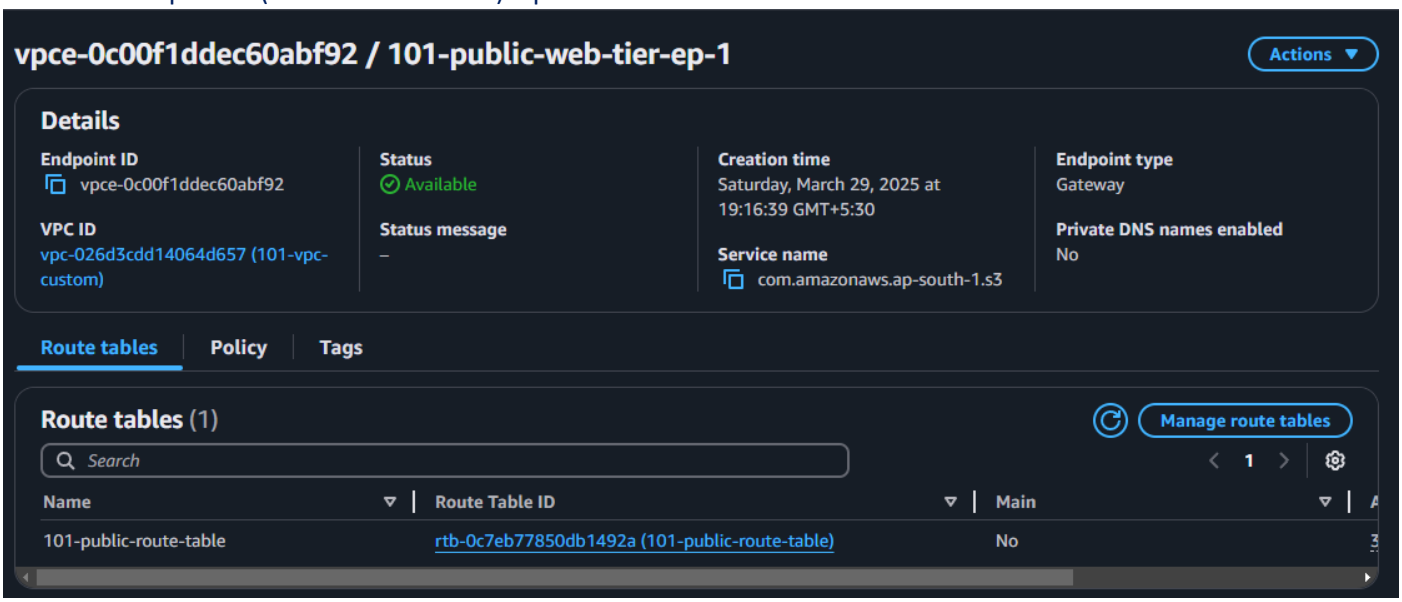
9.5. Security group of private db tier allows only TCP(3306) from app tier SG



10. Endpoints – VPC gateway for a secure private connection between subnet's and S3 – (Data won't be transferred via internet.



10.1. VPC endpoint – (Public subnet to S3) – public route table

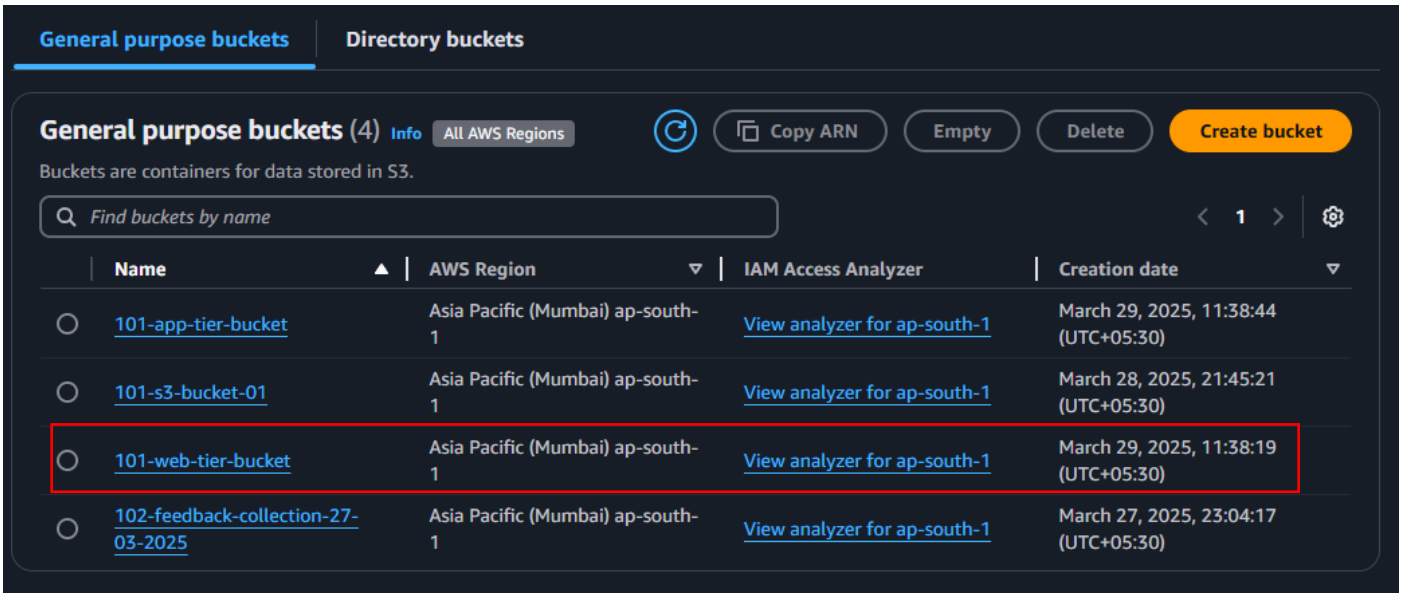


*Restrict the access by custom policy to access only a specific bucket

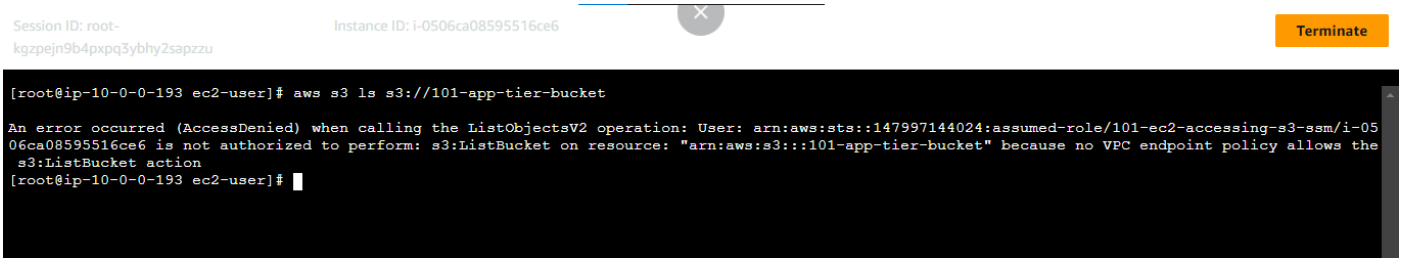
Policy

VPC endpoint policy controls access to the service

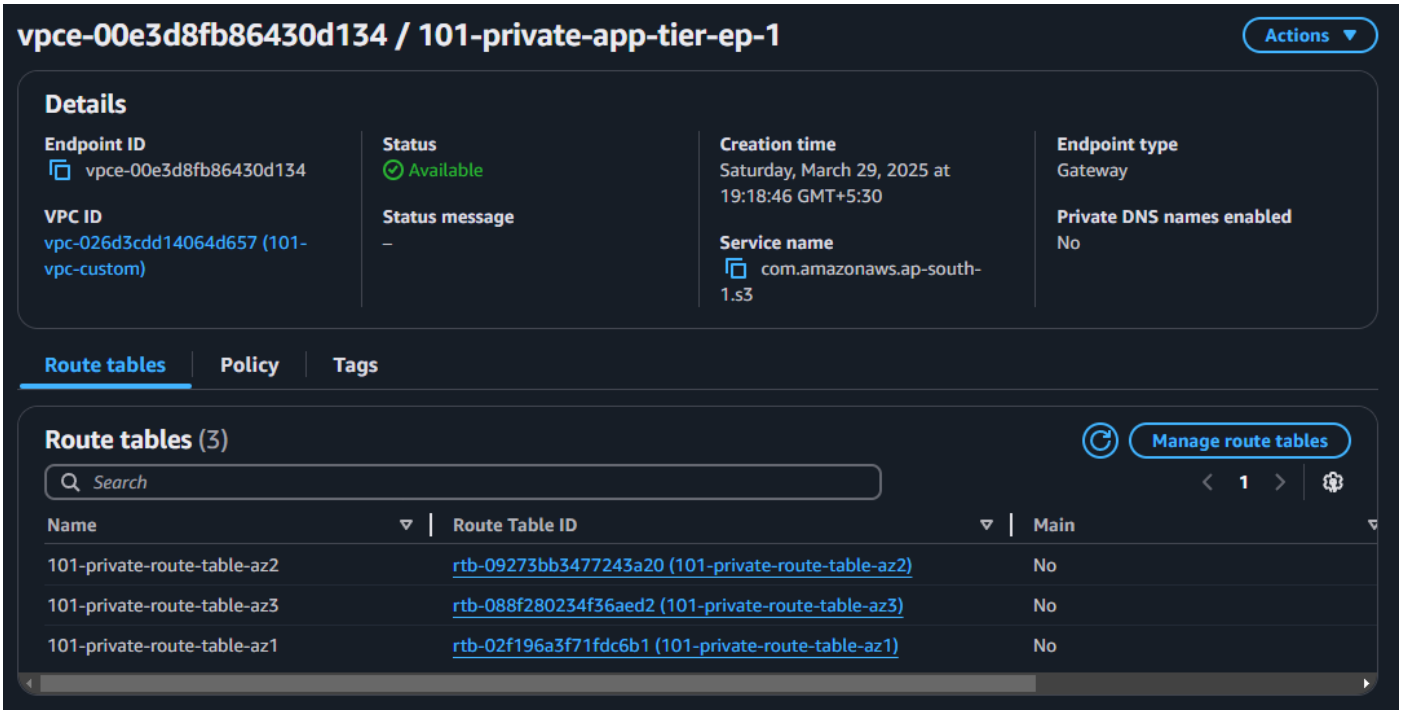
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::101-web-tier-bucket",
                "arn:aws:s3:::101-web-tier-bucket/*"
            ]
        }
    ]
}
```



Web tier access to app tier is not authorized, only can view web tier bucket as mentioned in policy



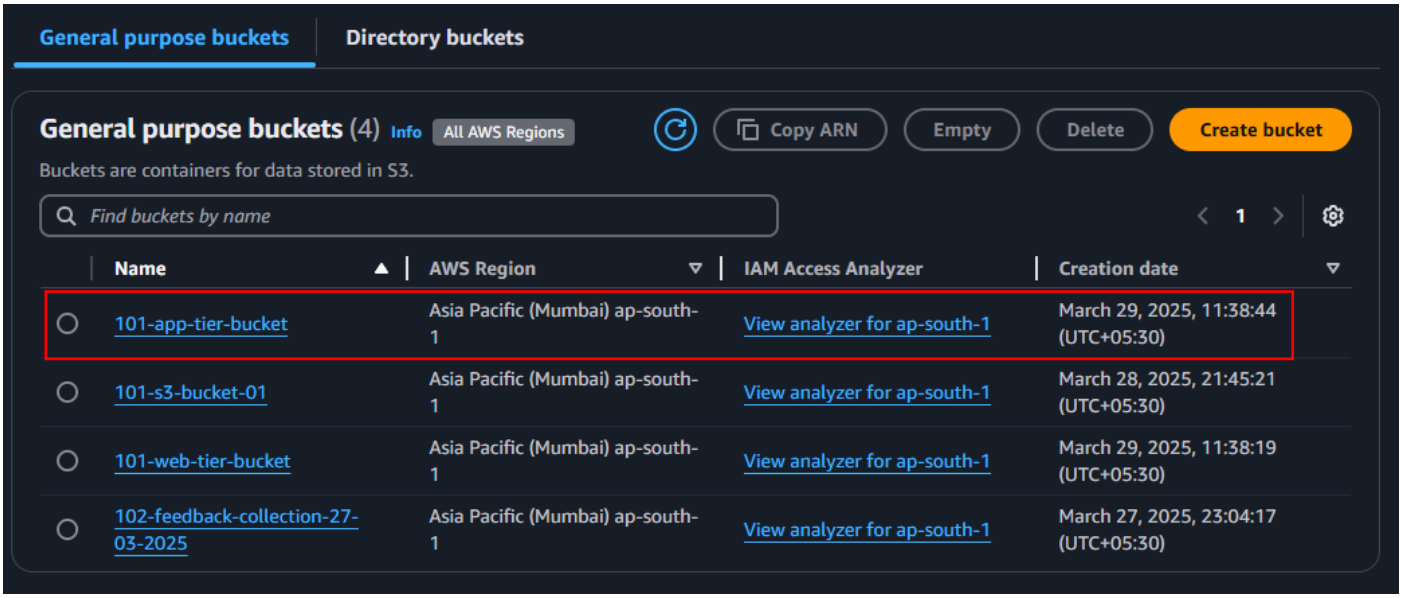
10.1. VPC endpoint – (Public subnet to S3) – public route table



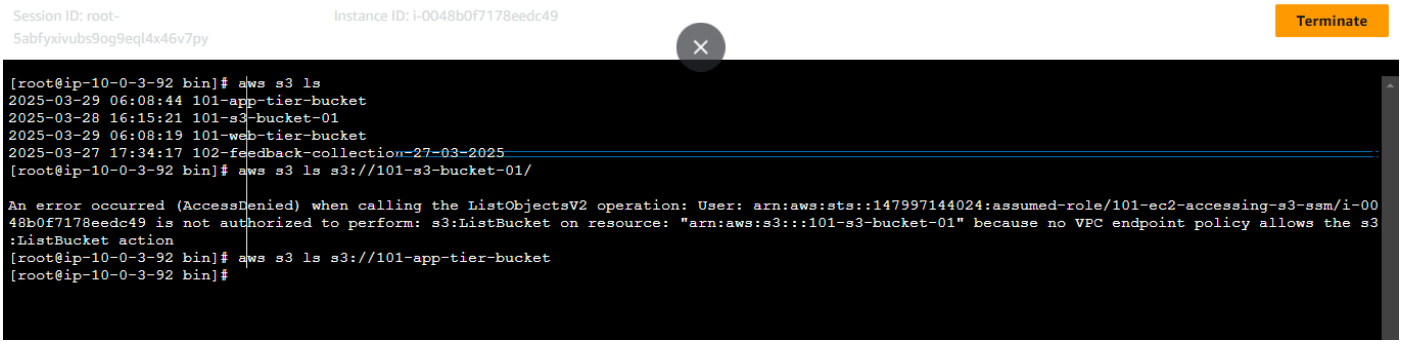
*Restrict the access by custom policy to access only a specific bucket

VPC endpoint policy controls access to the service

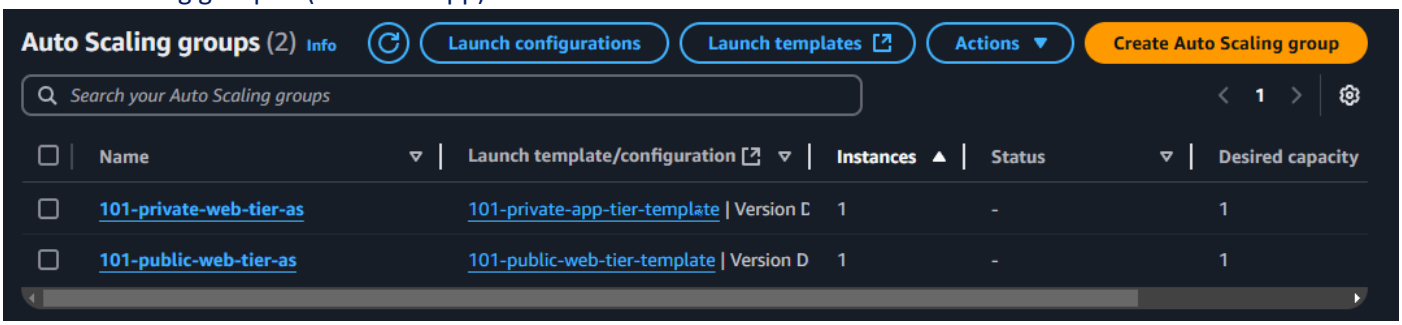
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::101-app-tier-bucket",
                "arn:aws:s3:::101-app-tier-bucket/*"
            ]
        }
    ]
}
```



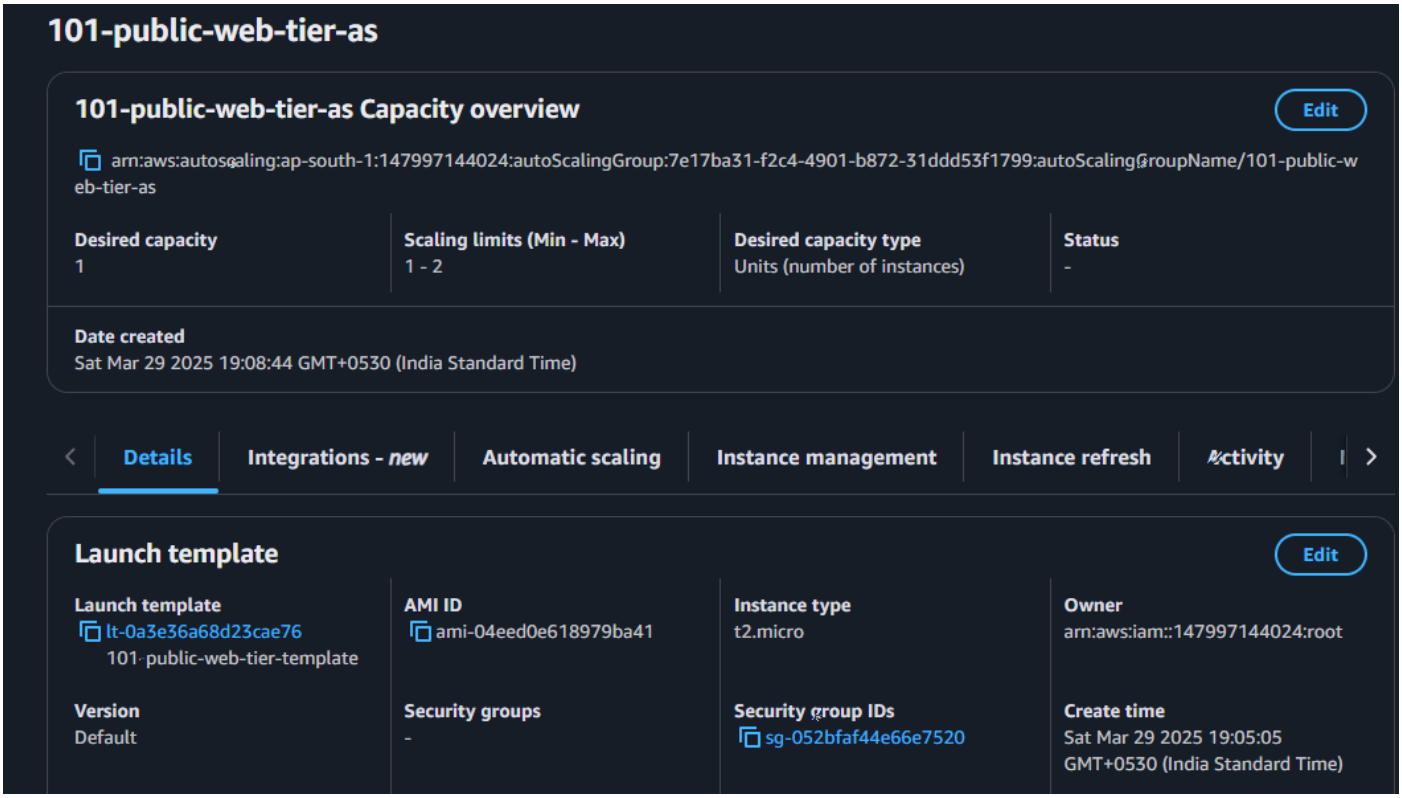
only can view app tier bucket as mentioned in policy



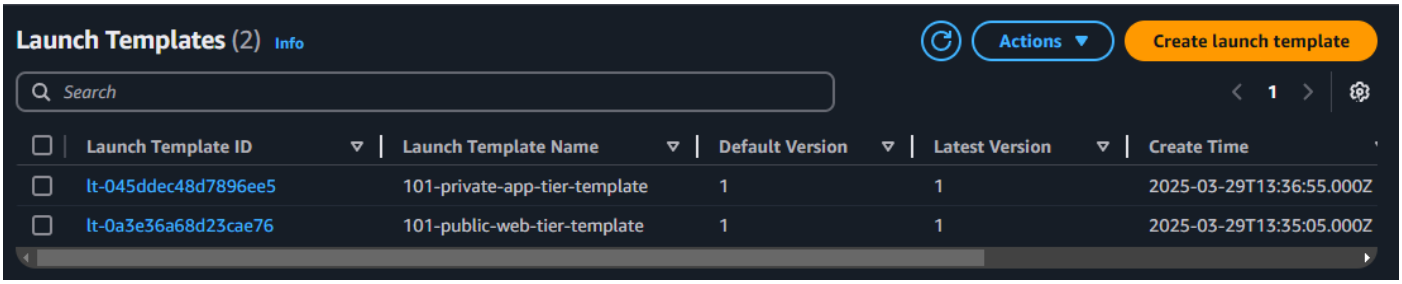
11. Auto scaling group -2 (Web and App)

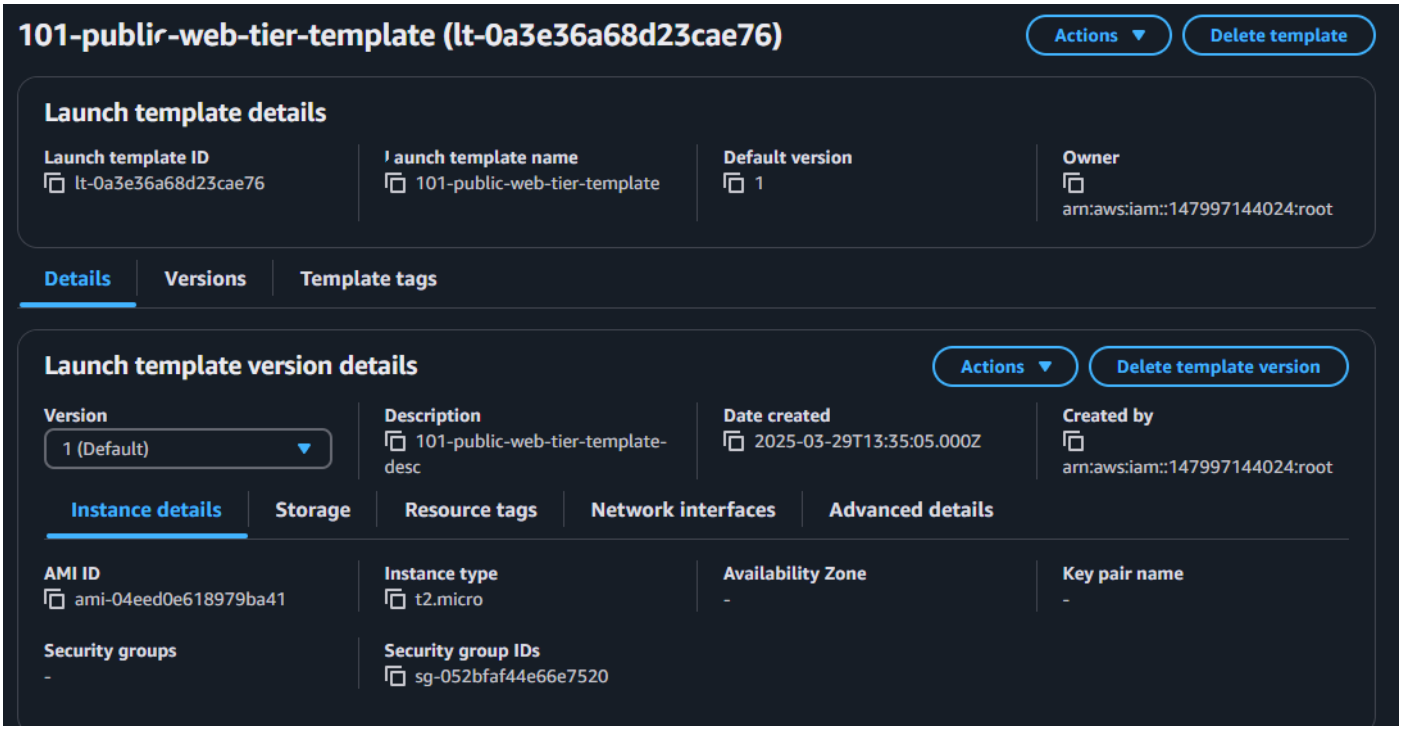


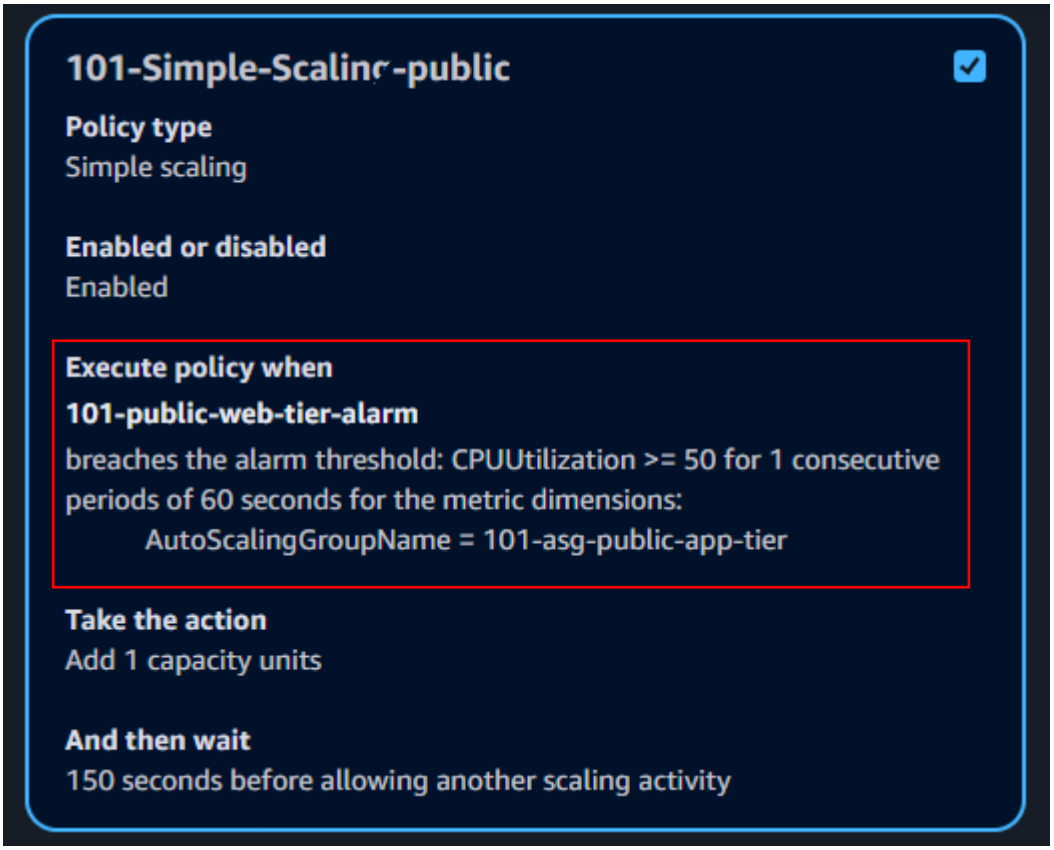
11.1 Public-web-tier



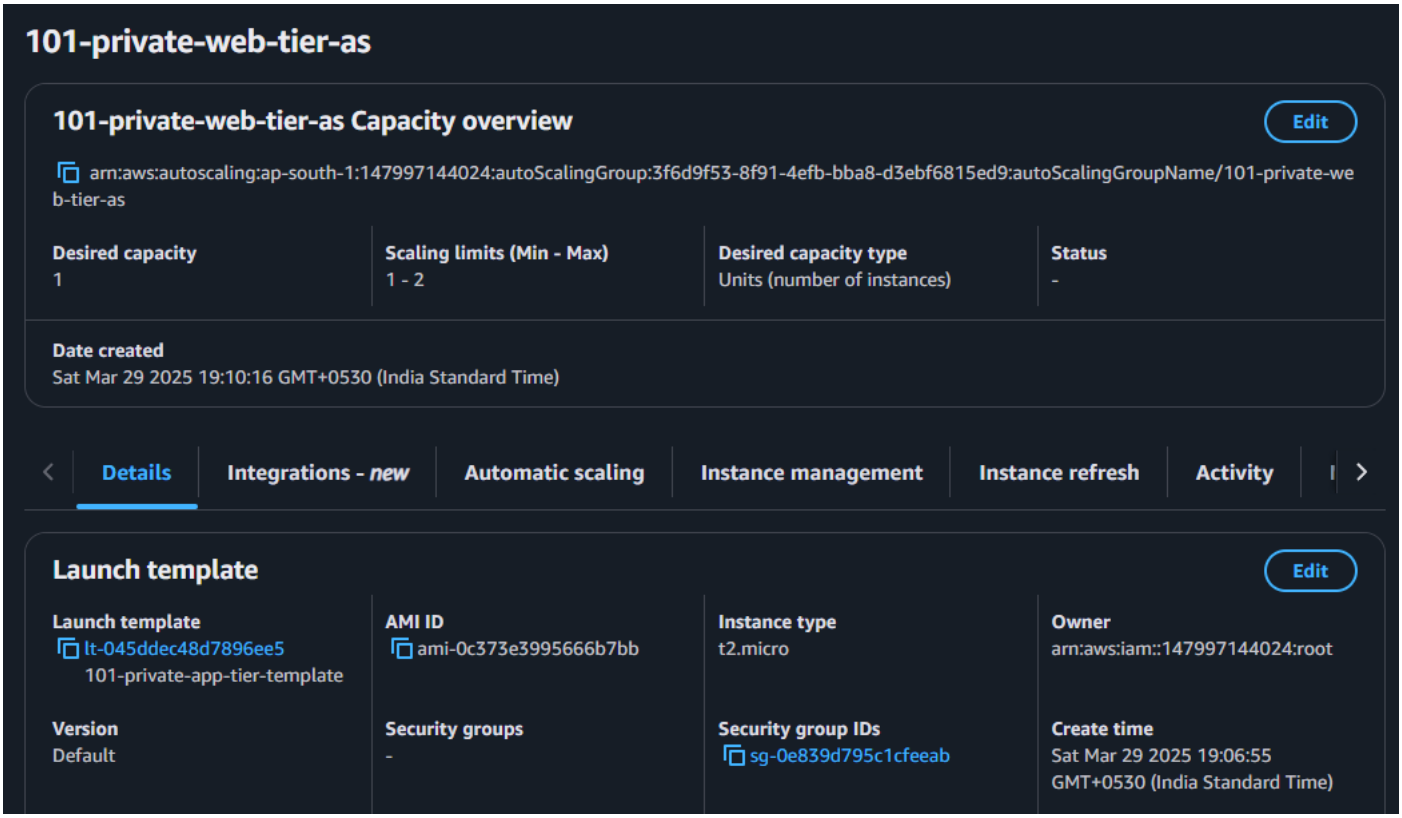
*Launch template



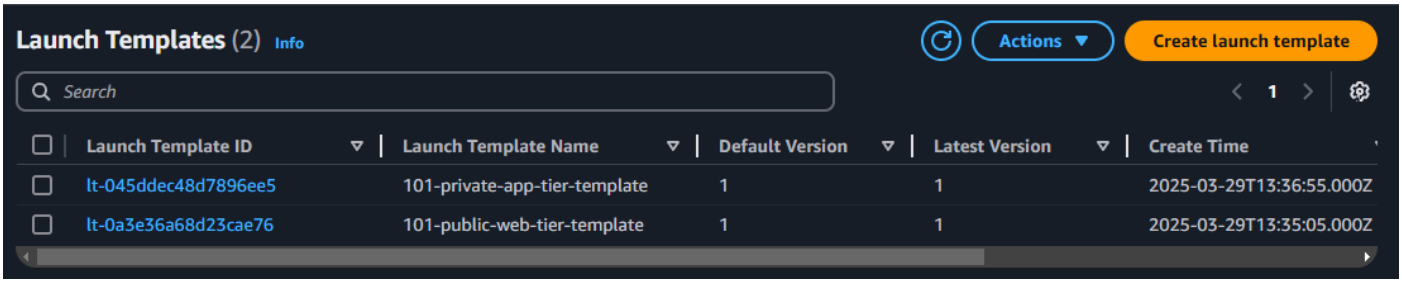

101-publir-web-tier-template (lt-0a3e36a68d23cae76)
Actions
Delete template
Launch template details
Launch template ID
lt-0a3e36a68d23cae76
Launch template name
101-public-web-tier-template
Default version
1
Owner
arn:aws:iam::147997144024:root
Details
Versions
Template tags
Launch template version details
Actions
Delete template version
Version
1 (Default)
Description
101-public-web-tier-template-desc
Date created
2025-03-29T13:35:05.000Z
Created by
arn:aws:iam::147997144024:root
Instance details
Storage
Resource tags
Network interfaces
Advanced details
AMI ID
ami-04eed0e618979ba41
Instance type
t2.micro
Availability Zone
-
Key pair name
-
Security groups
-
Security group IDs
sg-052bfaf44e66e7520

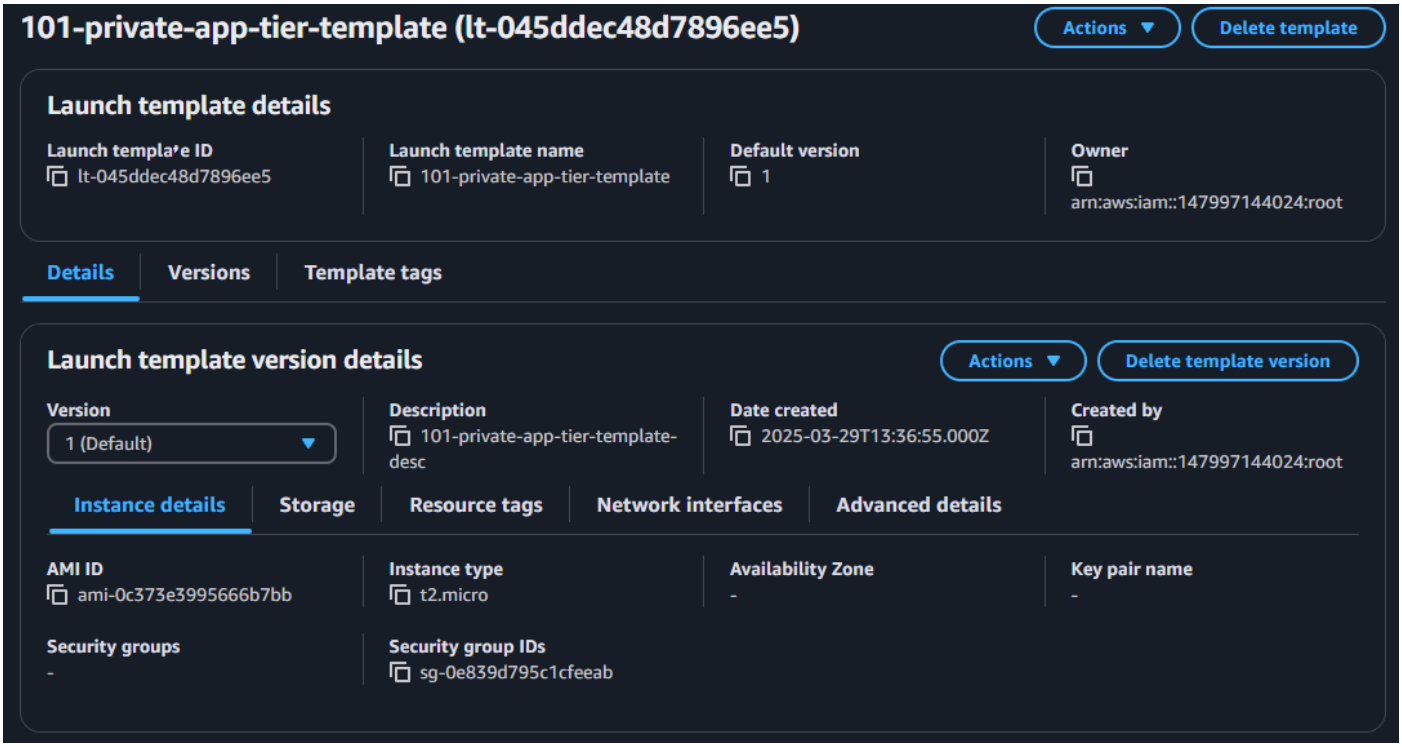

101-Simple-Scalinc-public
Policy type
Simple scaling
Enabled or disabled
Enabled
Execute policy when
101-public-web-tier-alarm
breaches the alarm threshold: CPUUtilization >= 50 for 1 consecutive periods of 60 seconds for the metric dimensions:
AutoScalingGroupName = 101-asg-public-app-tier
Take the action
Add 1 capacity units
And then wait
150 seconds before allowing another scaling activity

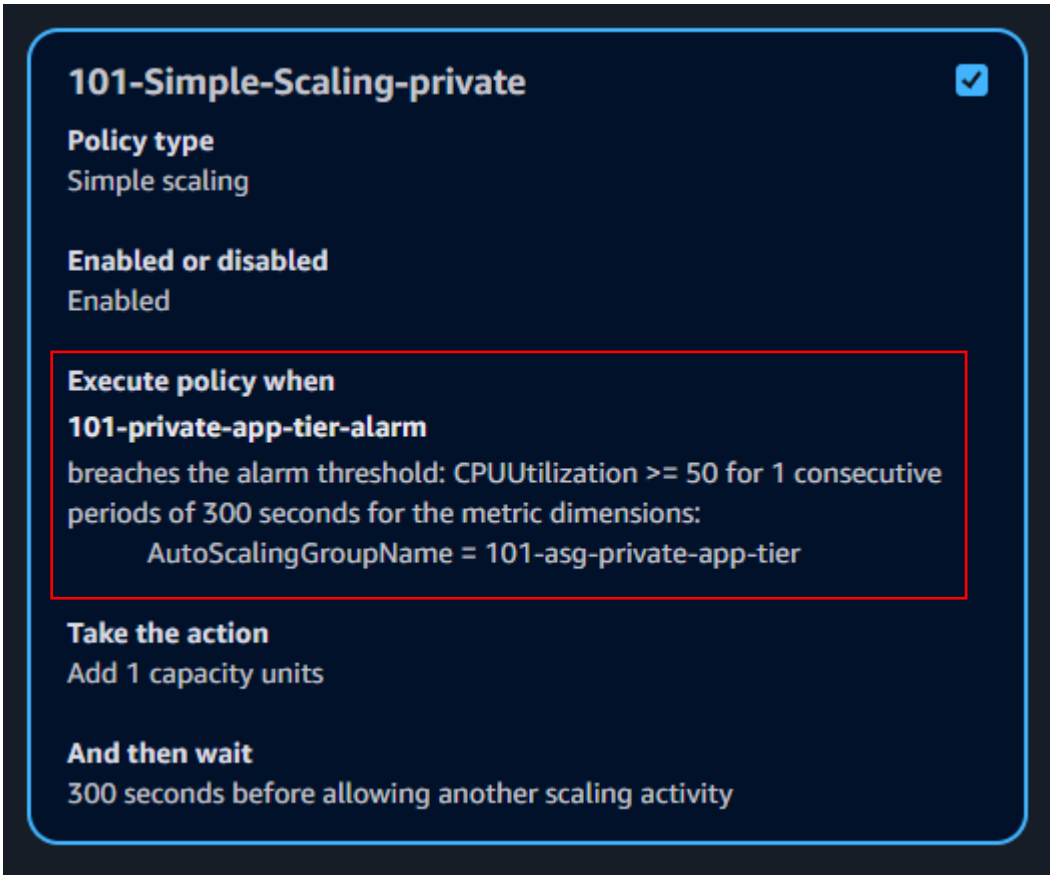
11.2 Private-app-tier (ignore web in below image - assigned name is incorrect)



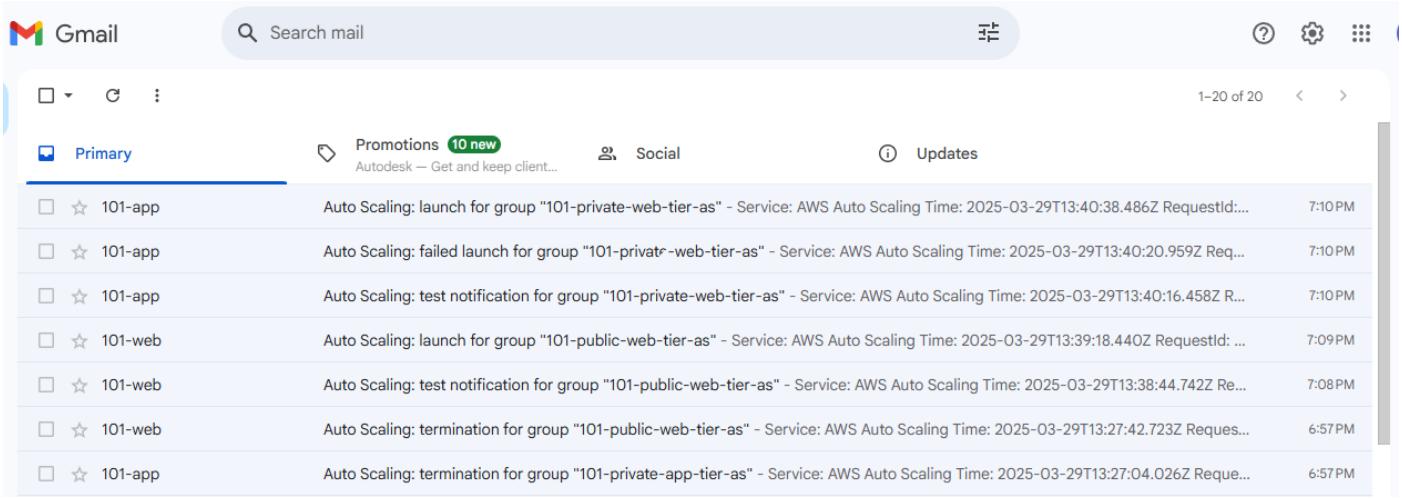
*Launch template



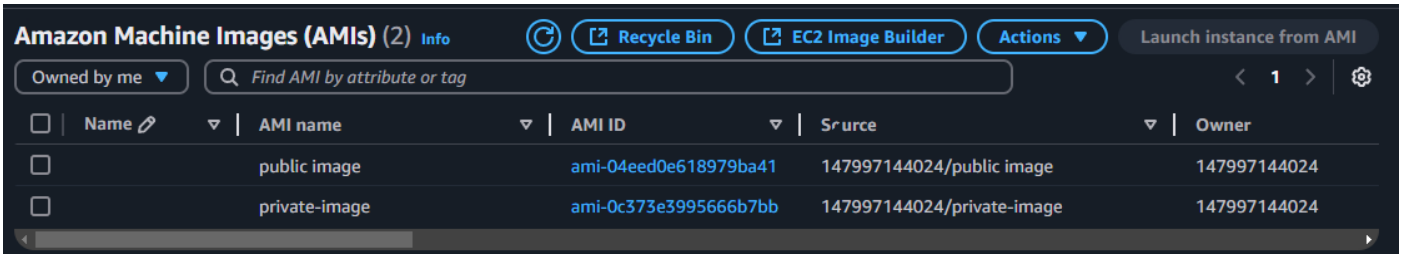

101-private-app-tier-template (lt-045ddec48d7896ee5)
Actions
Delete template
Launch template details
Launch templa*e ID
lt-045ddec48d7896ee5
Launch template name
101-private-app-tier-template
Default version
1
Owner
arn:aws:iam::147997144024:root
Details
Versions
Template tags
Launch template version details
Actions
Delete template version
Version
1 (Default)
Description
101-private-app-tier-template-desc
Date created
2025-03-29T13:36:55.000Z
Created by
arn:aws:iam::147997144024:root
Instance details
Storage
Resource tags
Network interfaces
Advanced details
AMI ID
ami-0c373e3995666b7bb
Instance type
t2.micro
Availability Zone
-
Key pair name
-
Security groups
-
Security group IDs
sg-0e839d795c1cfeeab


101-Simple-Scaling-private
Policy type
Simple scaling
Enabled or disabled
Enabled
Execute policy when
101-private-app-tier-alarm
breaches the alarm threshold: CPUUtilization >= 50 for 1 consecutive periods of 300 seconds for the metric dimensions:
AutoScalingGroupName = 101-asg-private-app-tier
Take the action
Add 1 capacity units
And then wait
300 seconds before allowing another scaling activity

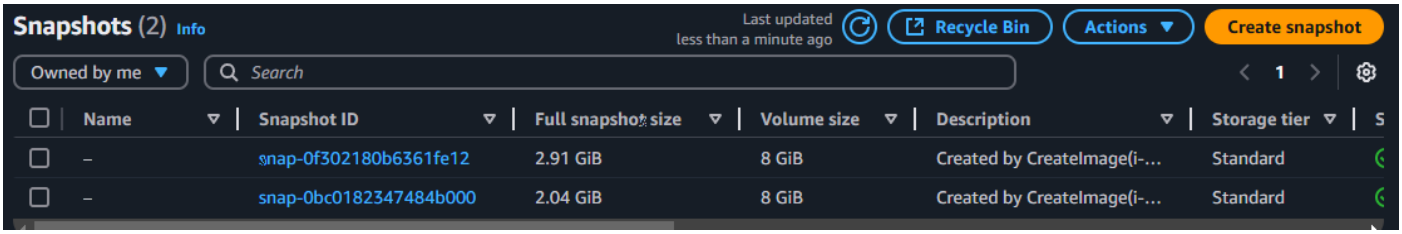
SNS – Topic enabled for each scaling activity performed.



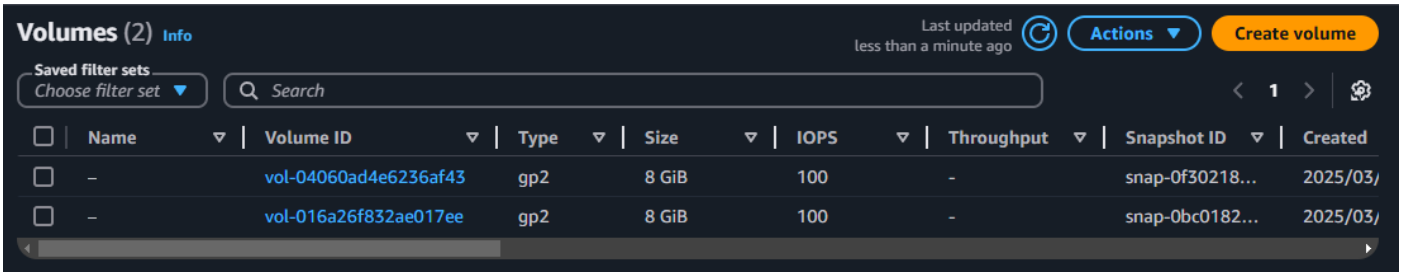
12. AMI – Autoscaling template was created by AMI (backedup by snapshots)



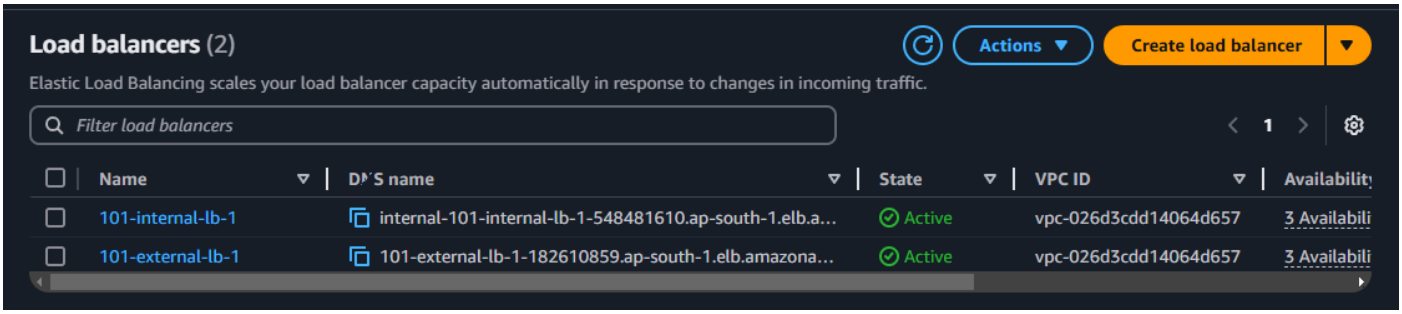
13 . Snapshot of AMI



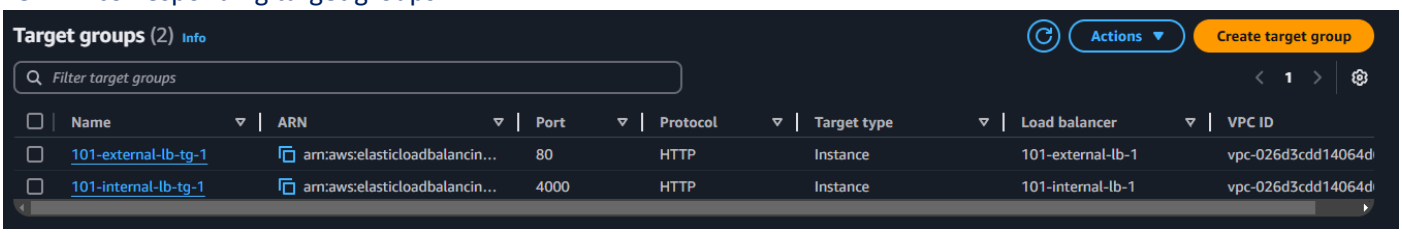
14 . Corresponding volume set of ec2 instance – public & private

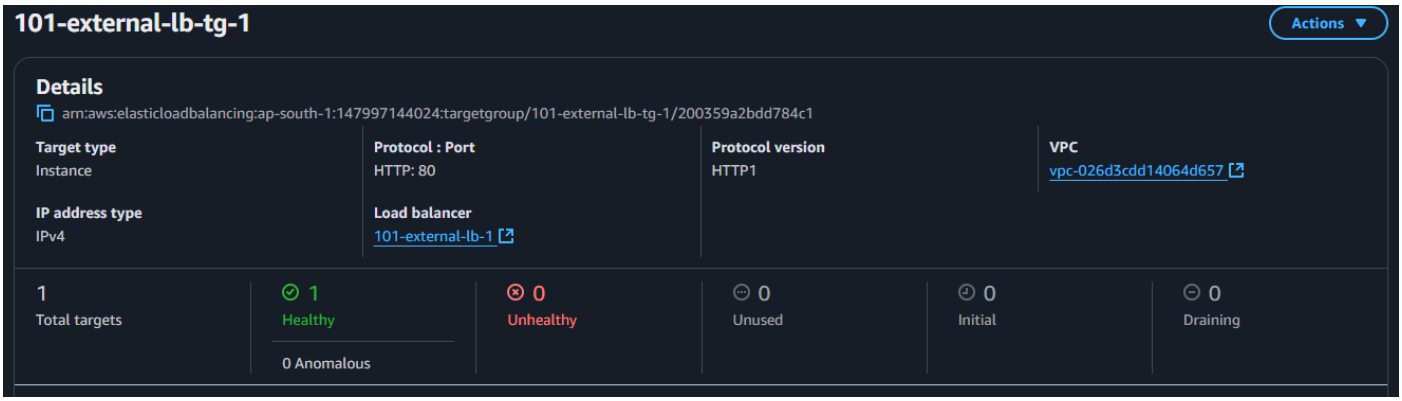


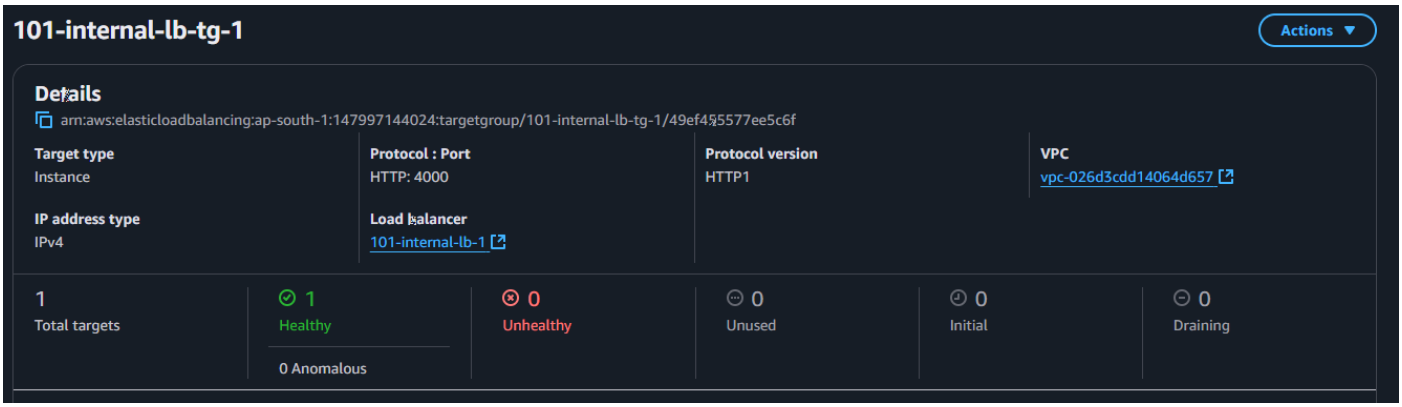
15. LB – internal & external



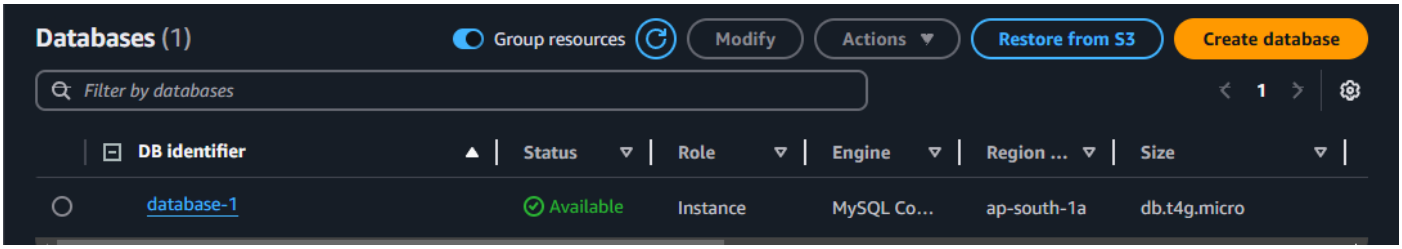
15.1 LB corresponding target groups

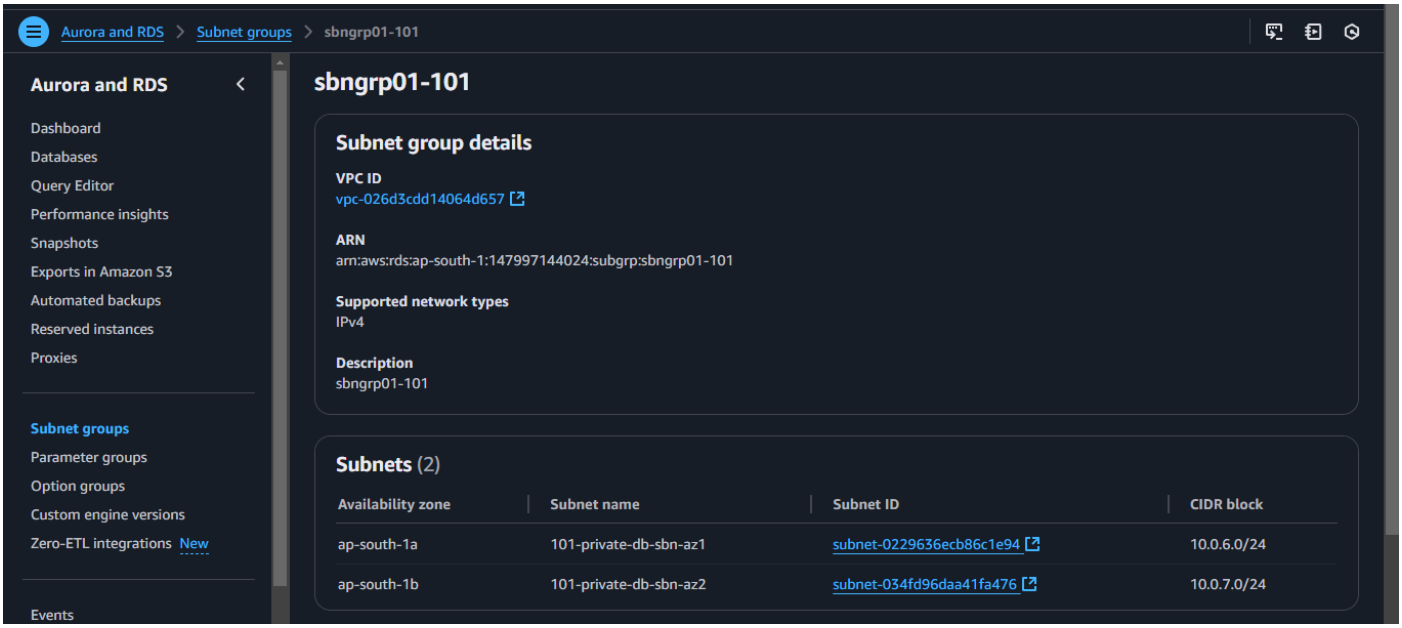






16. RDS database

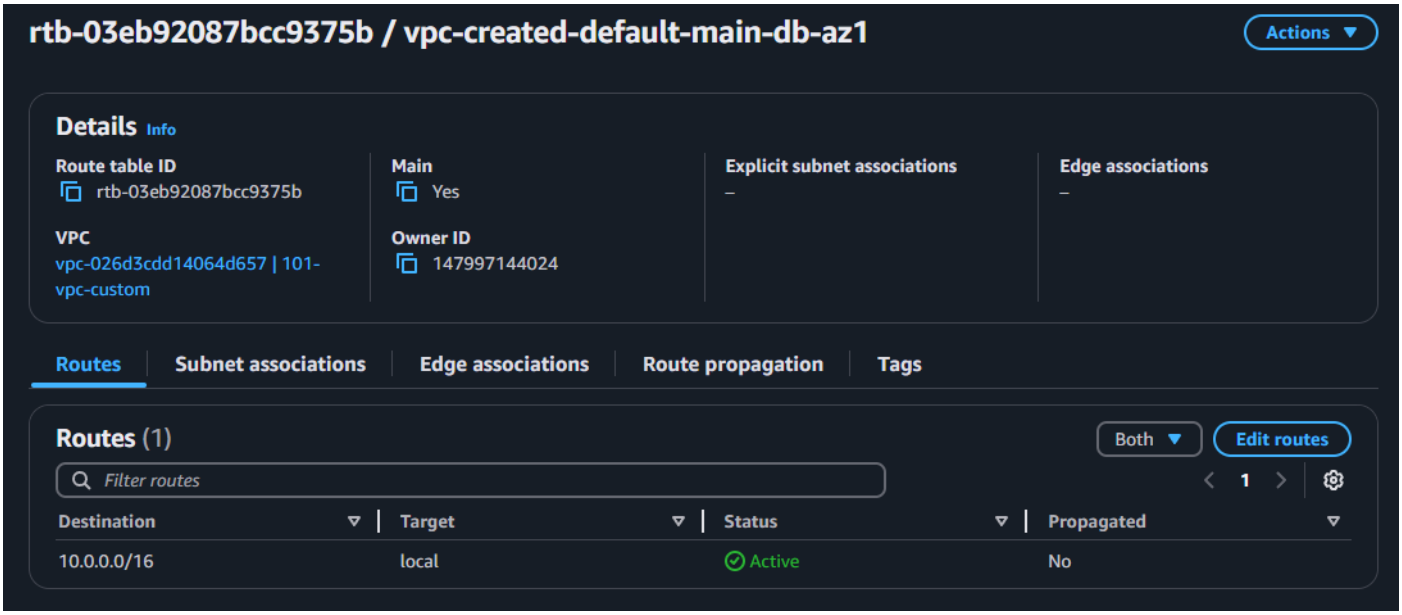




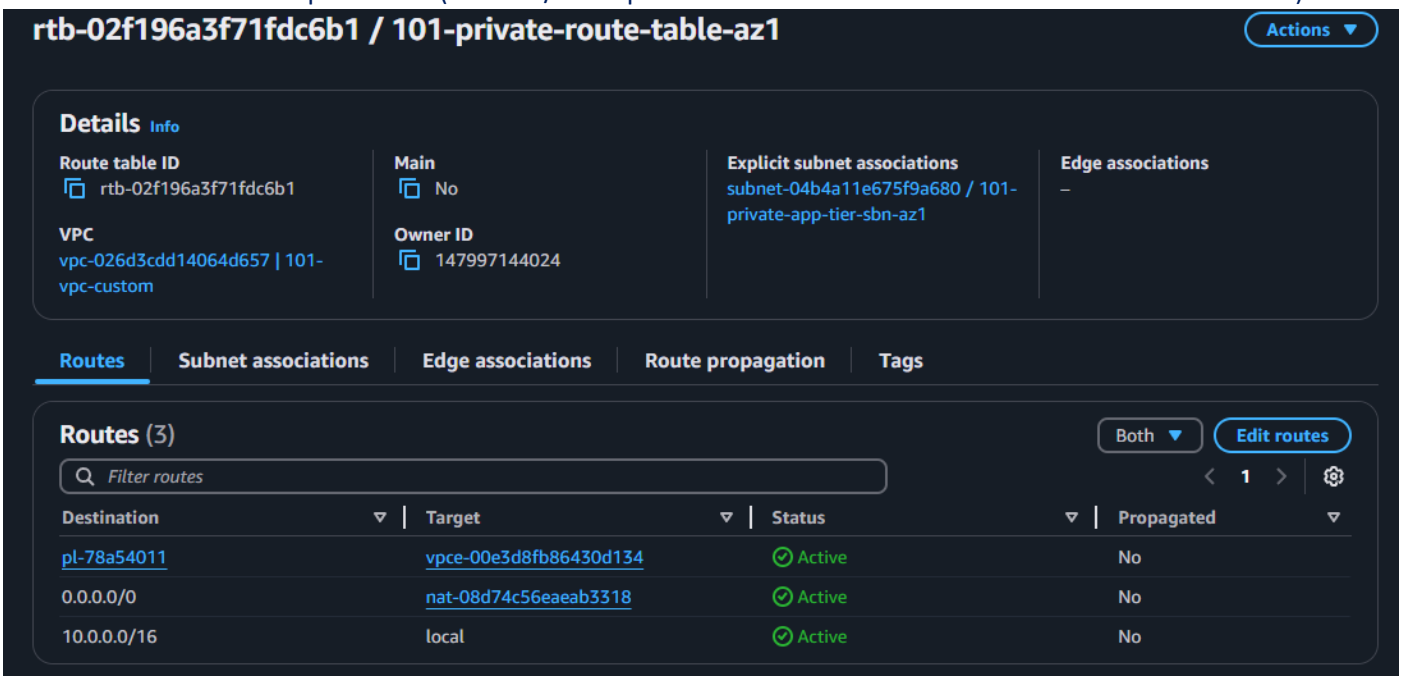
17. Route table configurations

17.1 Public route table common for all public az1, 2, 3(10.0.0.0/16 – vpc internal communication – we can remove this as well)

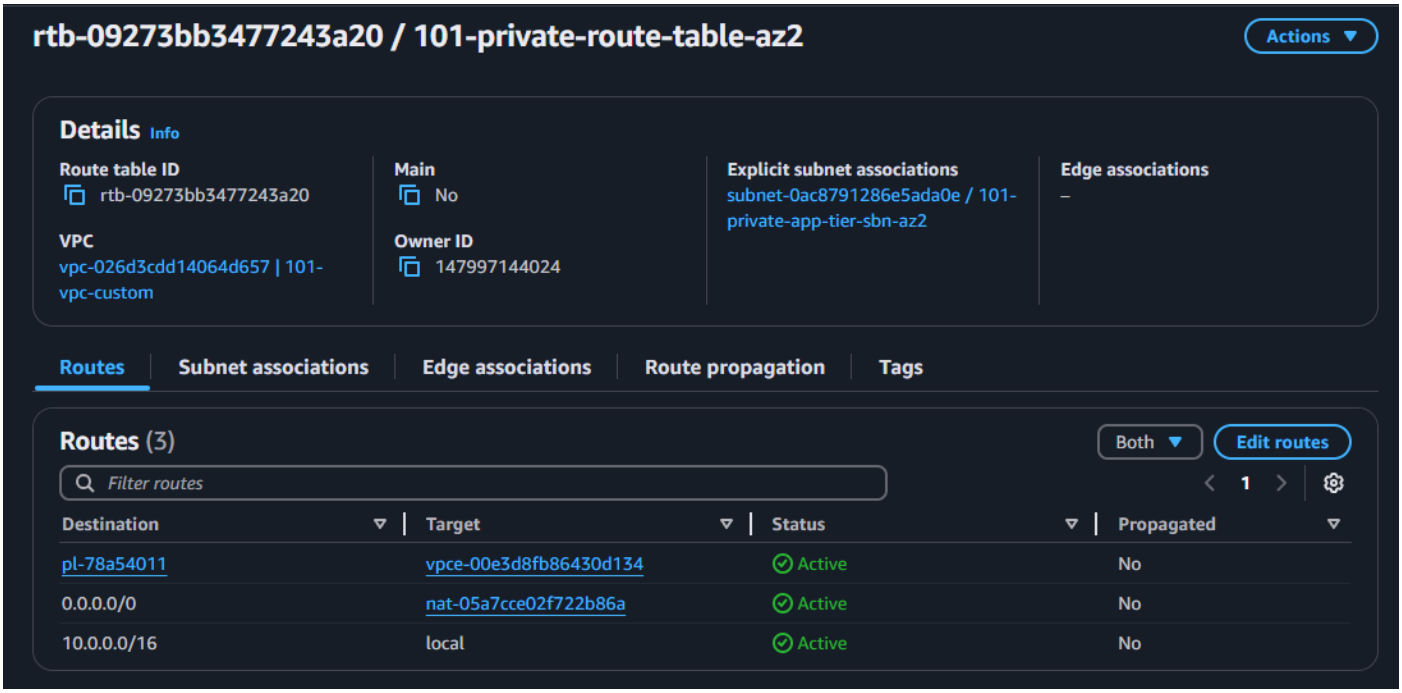
No subnet association just created when the VPC created



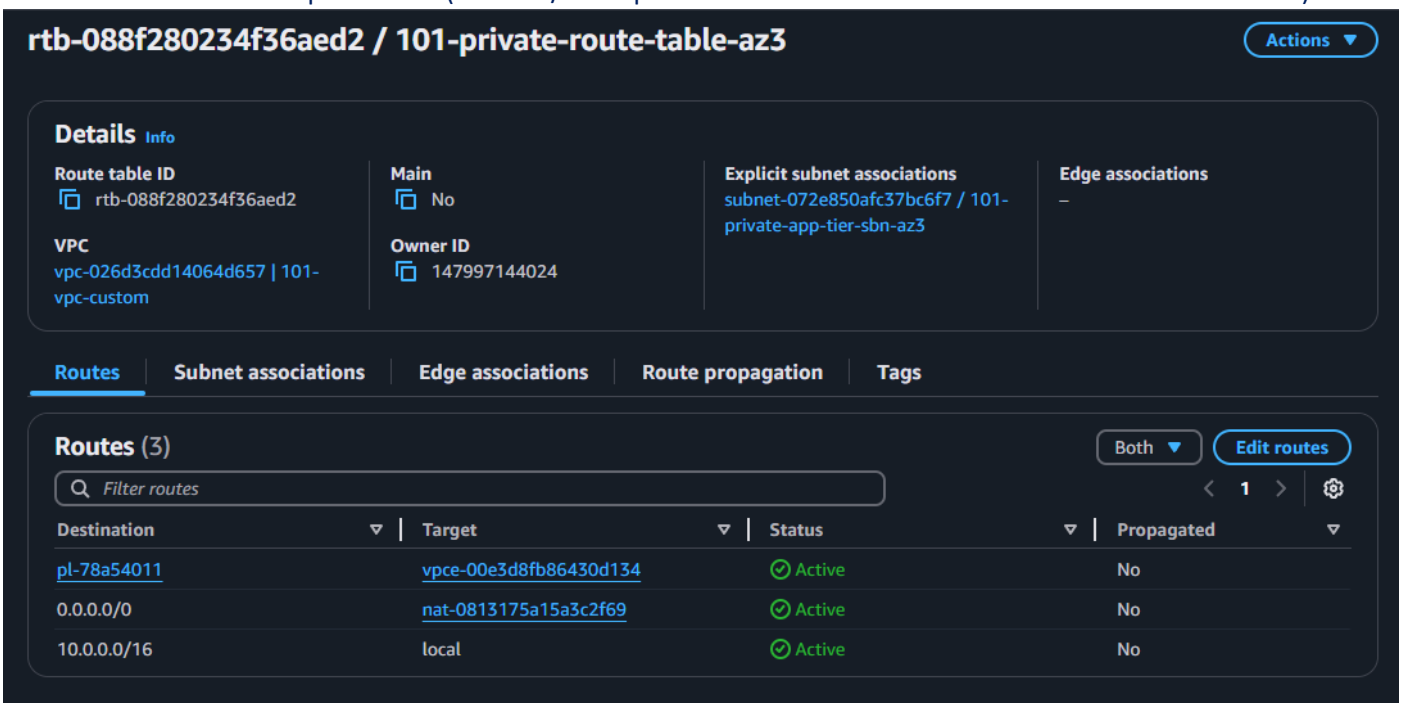
17.2 Private route table - private az1(10.0.0.0/16 – vpc internal communication – we can remove this as well)



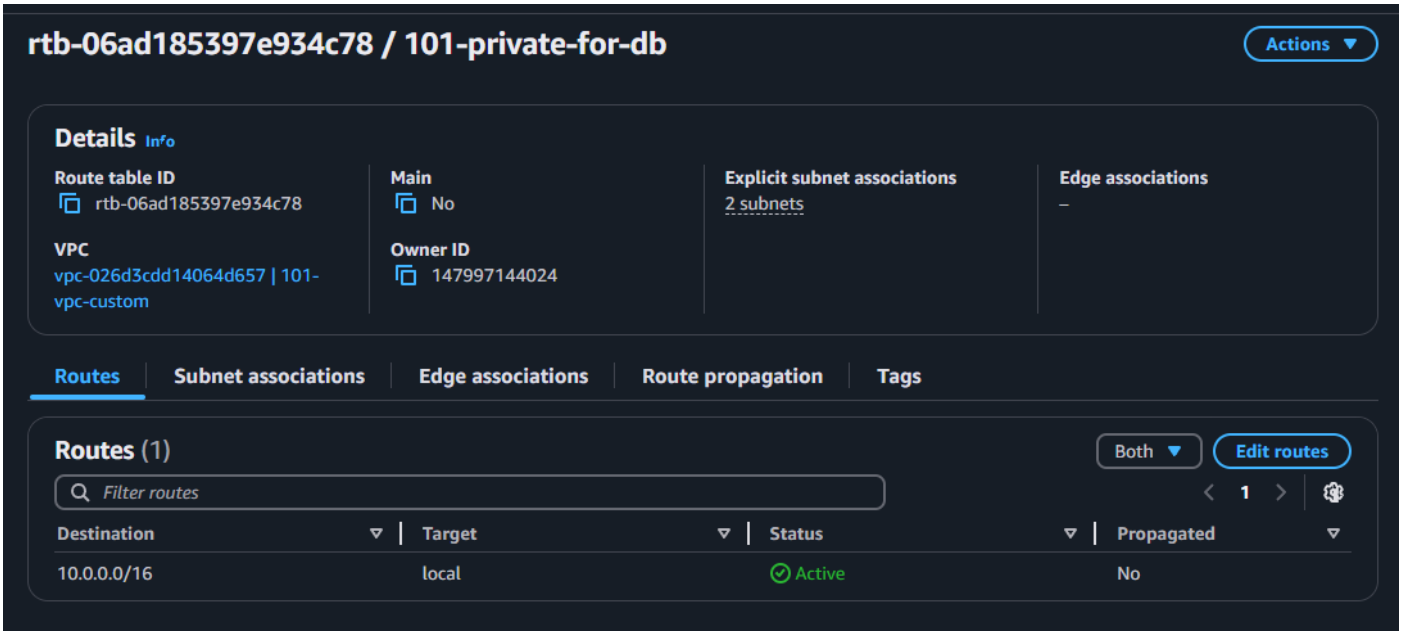
17.3 Private route table - private az2(10.0.0.0/16 – vpc internal communication – we can remove this as well)



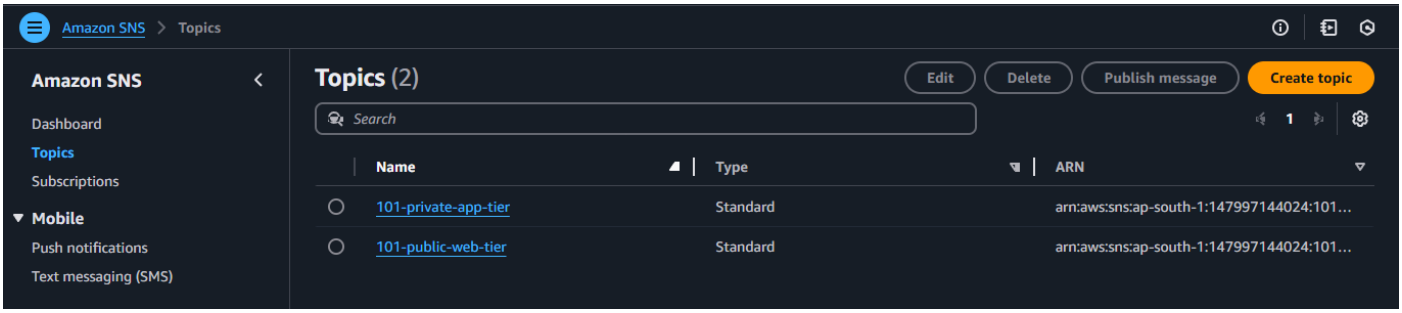
17.3 Private route table - private az3 (10.0.0.0/16 – vpc internal communication – we can remove this as well)



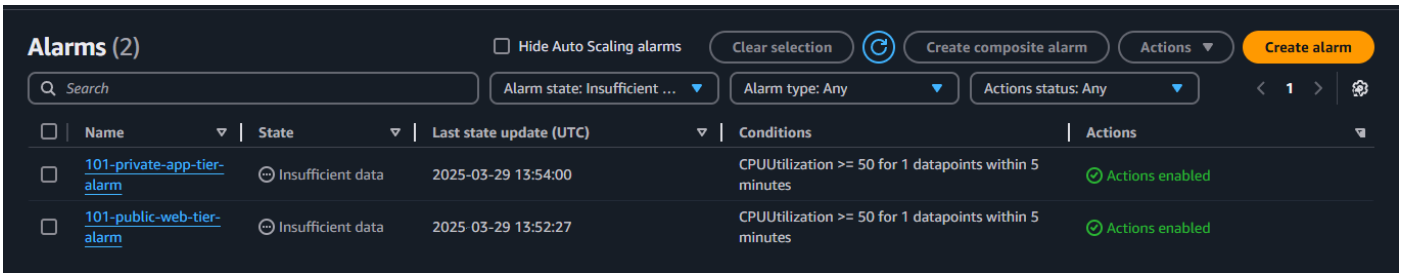
17.4 Private route table - private db – (No internet access) - (10.0.0.0/16 – vpc internal communication – we can remove this as well)



18. Topic & subcriptions



19. Cloud watch alarm with SNS enabled -



19.1 Alarm triggered SNS

ALARM: "101-public-app-tier-alarm" in Asia Pacific (Mumbai) Inbox ×

101-web <no-reply@sns.amazonaws.com> 12:03 AM (8 hours ago)
to me

You are receiving this email because your Amazon CloudWatch Alarm "101-public-app-tier-alarm" in the Asia Pacific (Mumbai) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [53.21942141769582 (29/03/25 18:32:00)] was greater than or equal to the threshold (50.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Saturday 29 March, 2025 18:33:56 UTC".

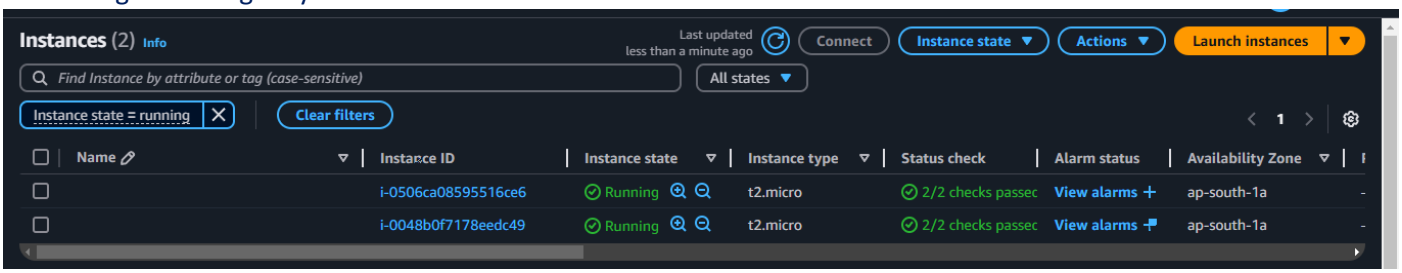
View this alarm in the AWS Management Console:
https://ap-south-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=ap-south-1#alarmsV2:alarm/101-public-app-tier-alarm

Alarm Details:
- Name: 101-public-app-tier-alarm
- Description: threshold attained
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [53.21942141769582 (29/03/25 18:32:00)] was greater than or equal to the threshold (50.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Saturday 29 March, 2025 18:33:56 UTC
- AWS Account: 147997144024
- Alarm Arn: arn:aws:cloudwatch:ap-south-1:147997144024:alarm:101-public-app-tier-alarm

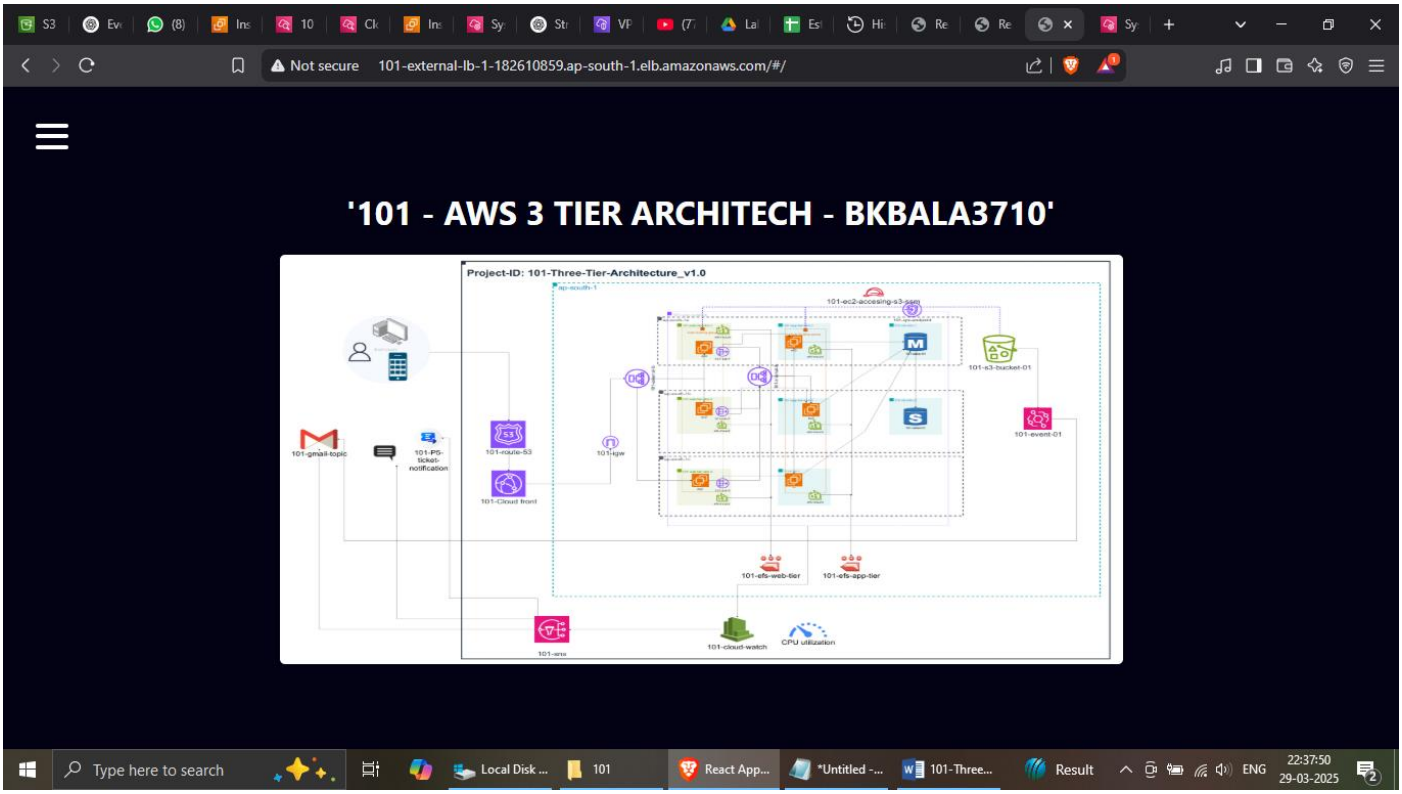
Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 50.0 for at least 1 of the last 1 period(s) of 60 seconds.

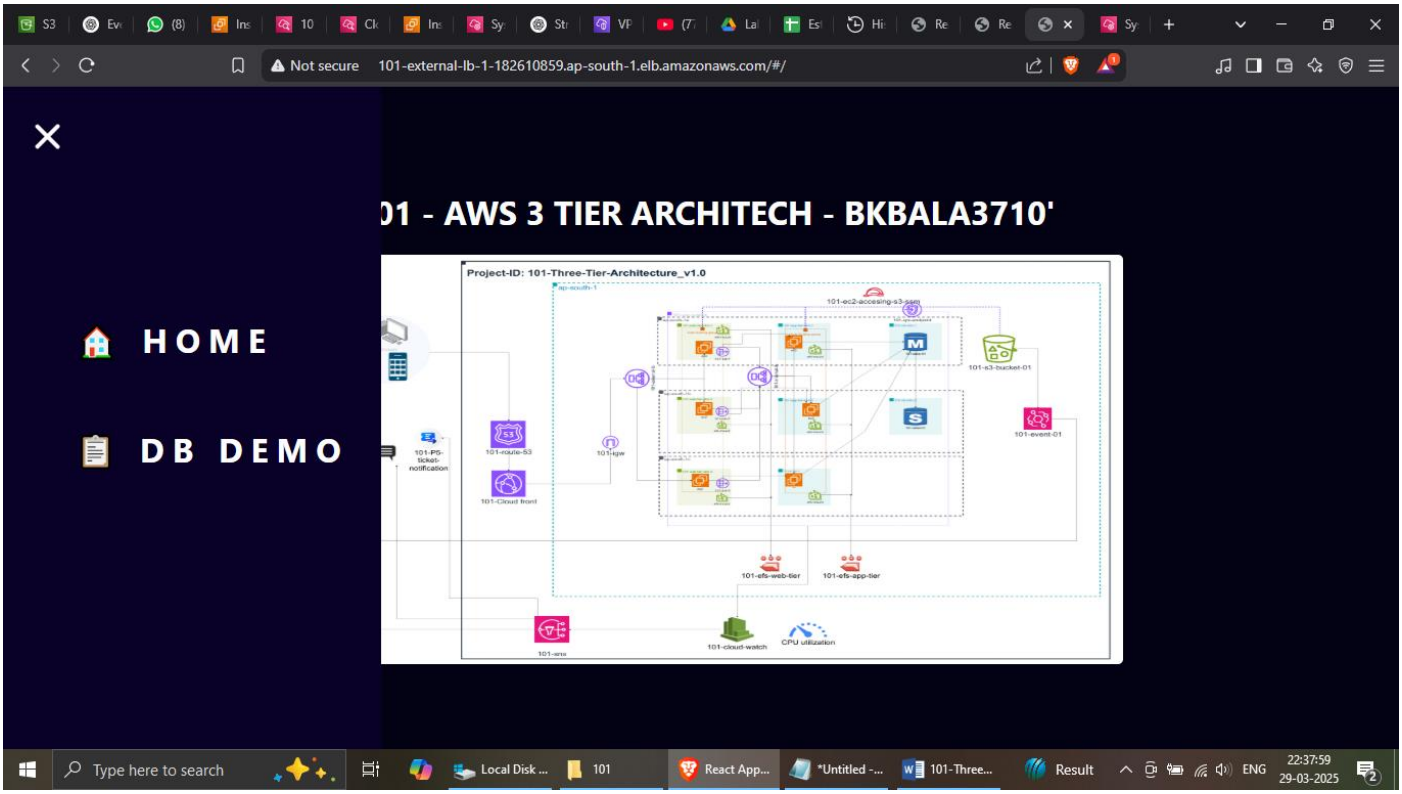
Monitored Metric:

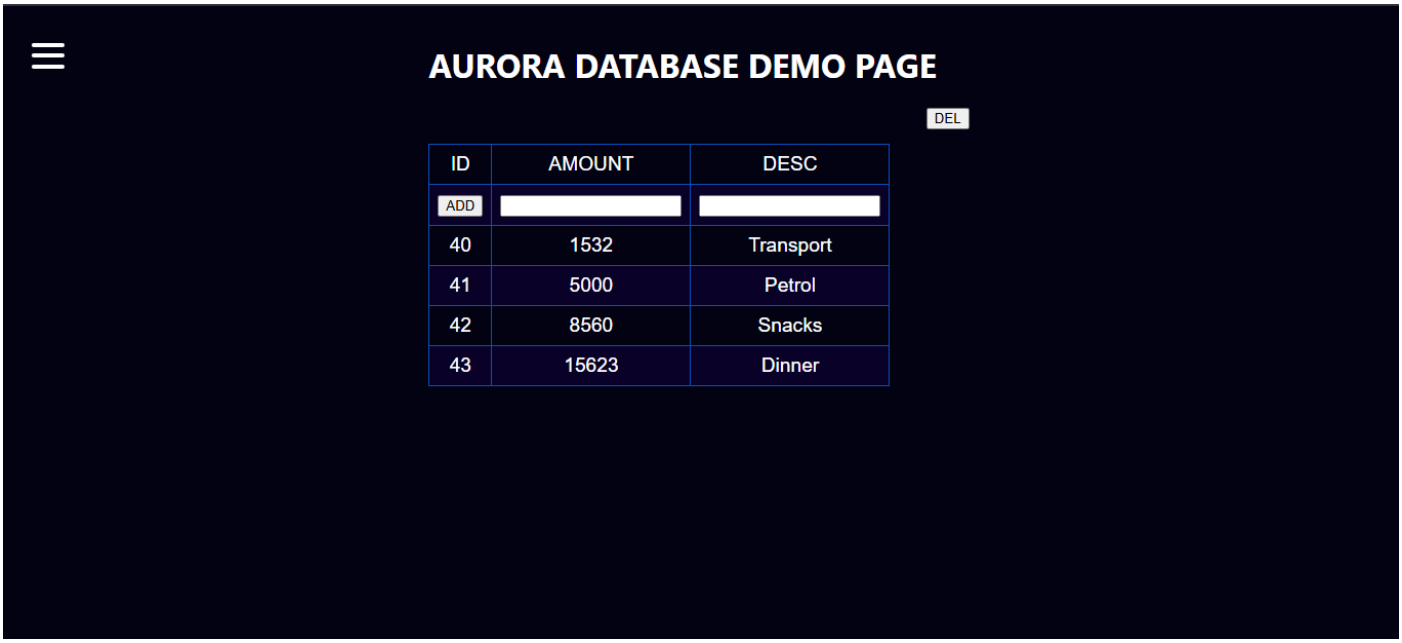
19. EC2 right running only 2 instance

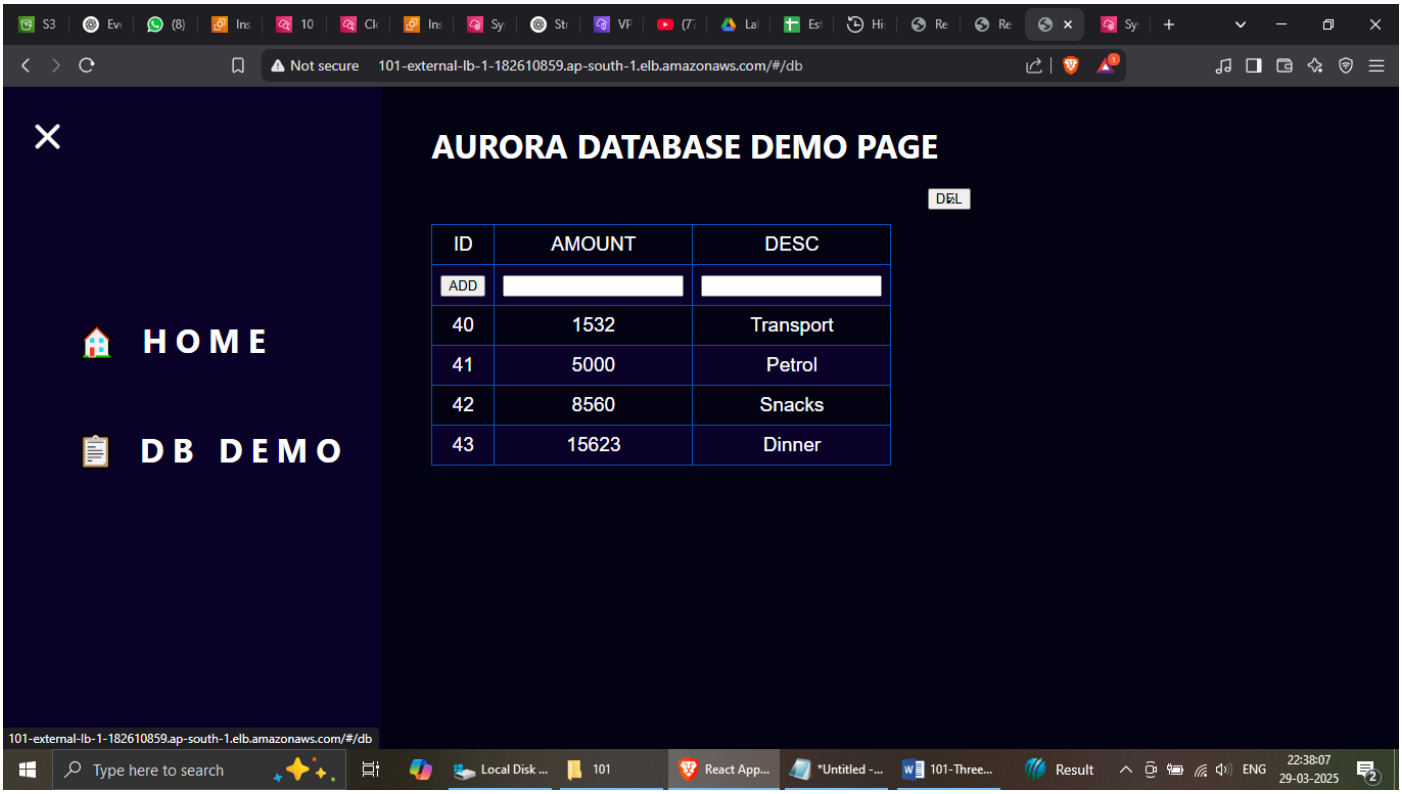


20. Demo

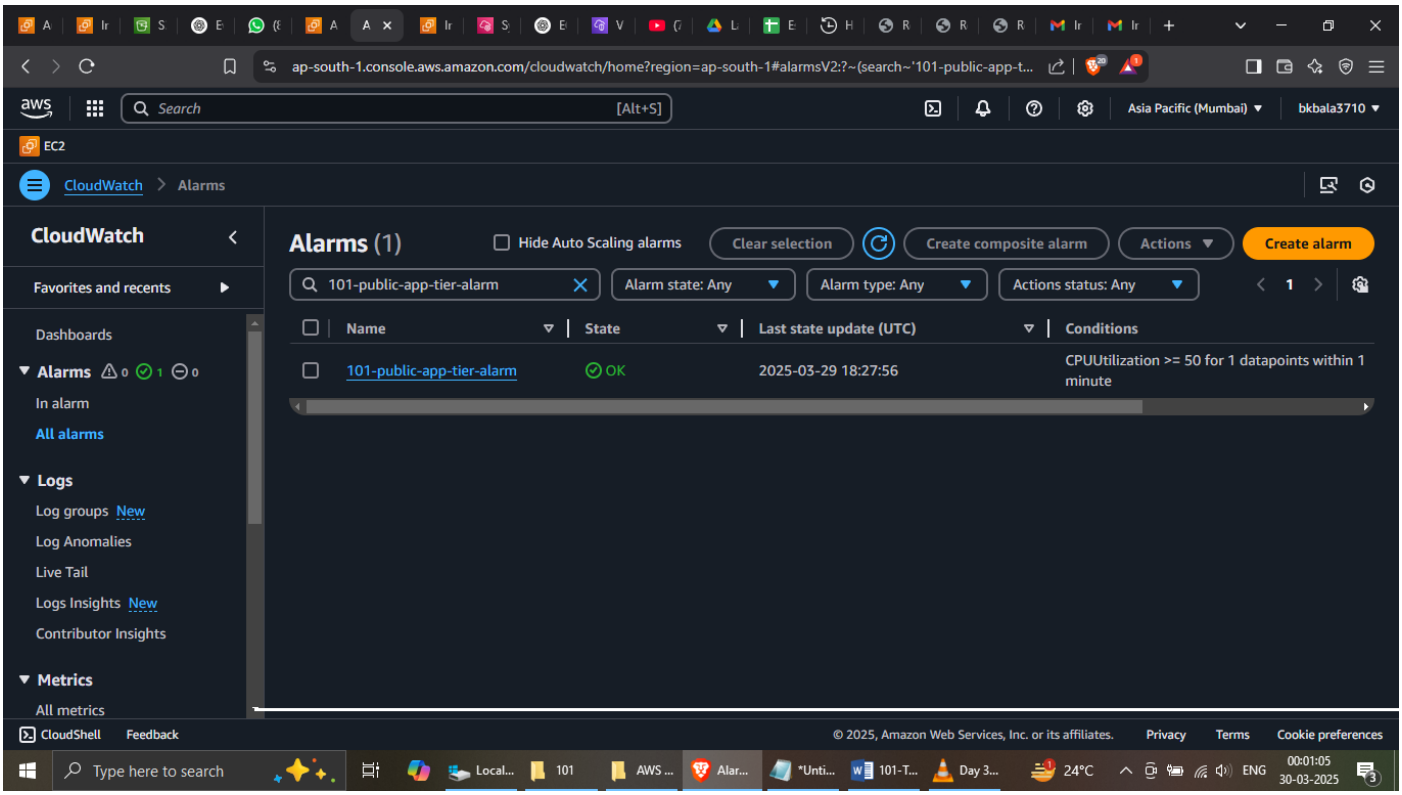

Not secure
101-external-lb-1-182610859.ap-south-1.elb.amazonaws.com/#/
'101 - AWS 3 TIER ARCHITECH - BKBALA3710'
Project-ID: 101-Three-Tier-Architecture_v1.0
Type here to search
Local Disk ...
101
React App...
*Untitled -...
101-Three...
Result
ENG
22:37:50
29-03-2025


Not secure
101-external-lb-1-182610859.ap-south-1.elb.amazonaws.com/#/
HOME
DB DEMO
01 - AWS 3 TIER ARCHITECH - BKBALA3710'
Project-ID: 101-Three-Tier-Architecture_v1.0
Type here to search
Local Disk ...
101
React App...
*Untitled -...
101-Three...
Result
ENG
22:37:59
29-03-2025


AURORA DATABASE DEMO PAGE
DEL
ID
AMOUNT
DESC
ADD
40
1532
Transport
41
5000
Petrol
42
8560
Snacks
43
15623
Dinner


Not secure
101-external-lb-1-182610859.ap-south-1.elb.amazonaws.com/#/db
AURORA DATABASE DEMO PAGE
DEL
ID
AMOUNT
DESC
ADD
40
1532
Transport
41
5000
Petrol
42
8560
Snacks
43
15623
Dinner
HOME
DB DEMO
101-external-lb-1-182610859.ap-south-1.elb.amazonaws.com/#/db
Type here to search
Local Disk ...
101
React App...
*Untitled -...
101-Three...
Result
ENG
22:38:07
29-03-2025

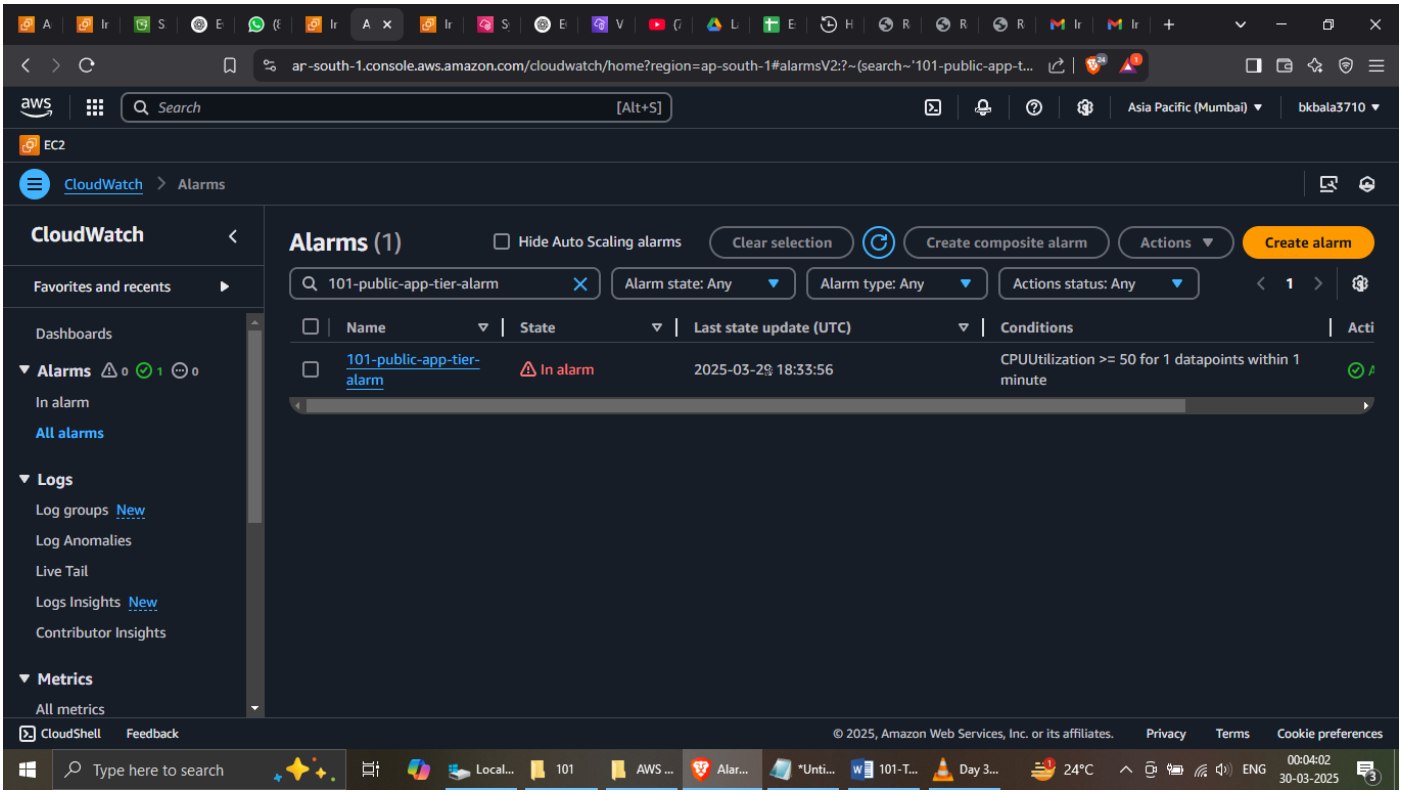
21. Initially – CPU utliization was below 50% of public ec2, measuring CPU utilization of auto scaling group is the best practice, but due to time constraint – I am setted up with ec2 public CPU utilization for quick alarm trigger…



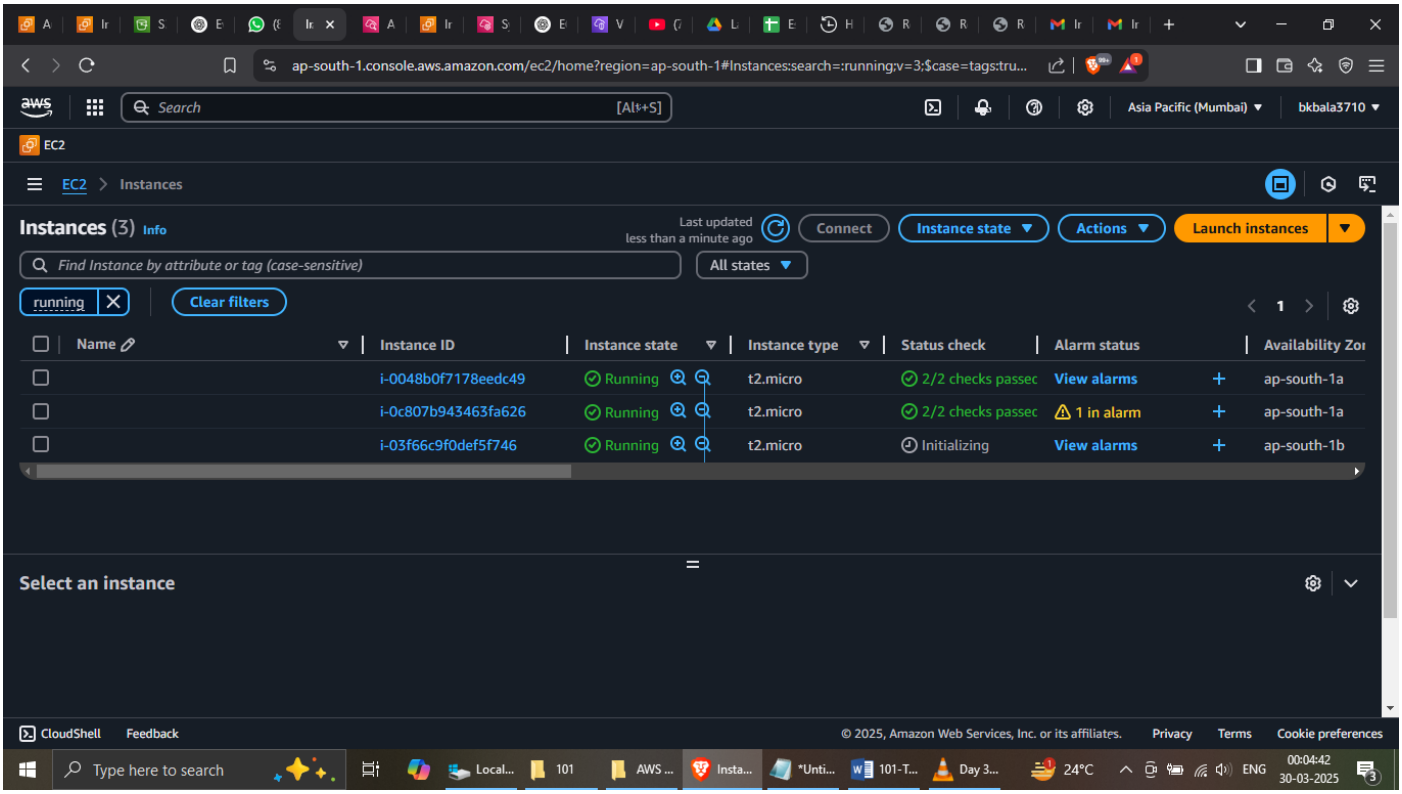
21.1. Enabling stress cmd in public ec2 to trigger alarm – (just as drill practice)

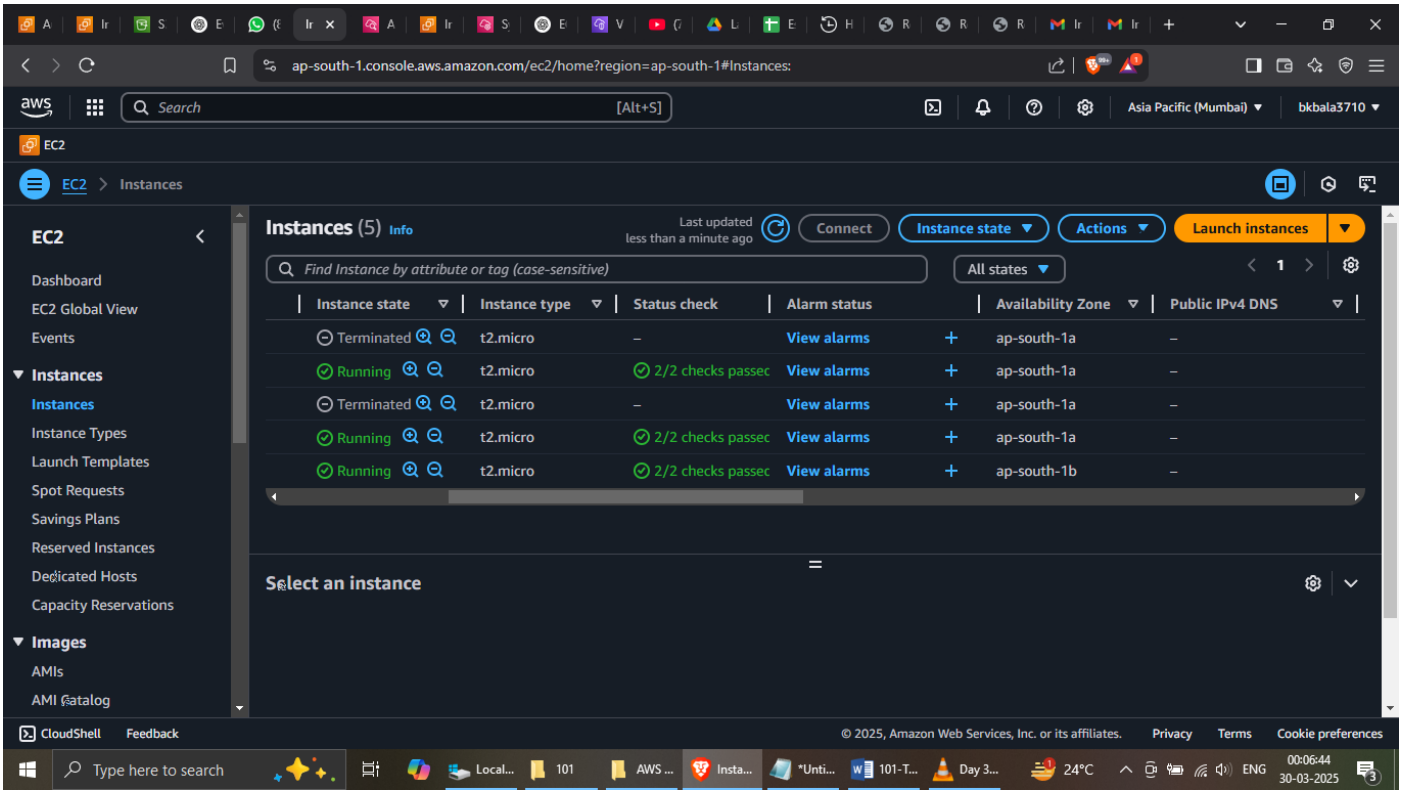
```
sh-4.2$ sudo su
[root@ip-10-0-0-193 bin]# pwd
/usr/bin
[root@ip-10-0-0-193 bin]# cd ..
[root@ip-10-0-0-193 usr]# pwd
/usr
[root@ip-10-0-0-193 usr]# cd /home/ec2_user
bash: cd: /home/ec2_user: No such file or directory
[root@ip-10-0-0-193 usr]# cd /home/ec2-user
[root@ip-10-0-0-193 ec2-user]# pwd
/home/ec2-user
[root@ip-10-0-0-193 ec2-user]# sudo dnf install stress -y
```

*Threshold of 50% attained – alarm triggered

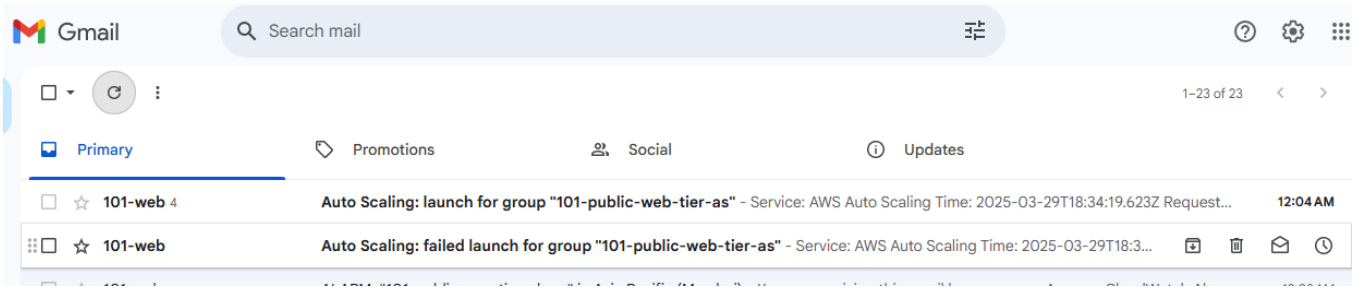


*Auto scaling performed as a result of alarm

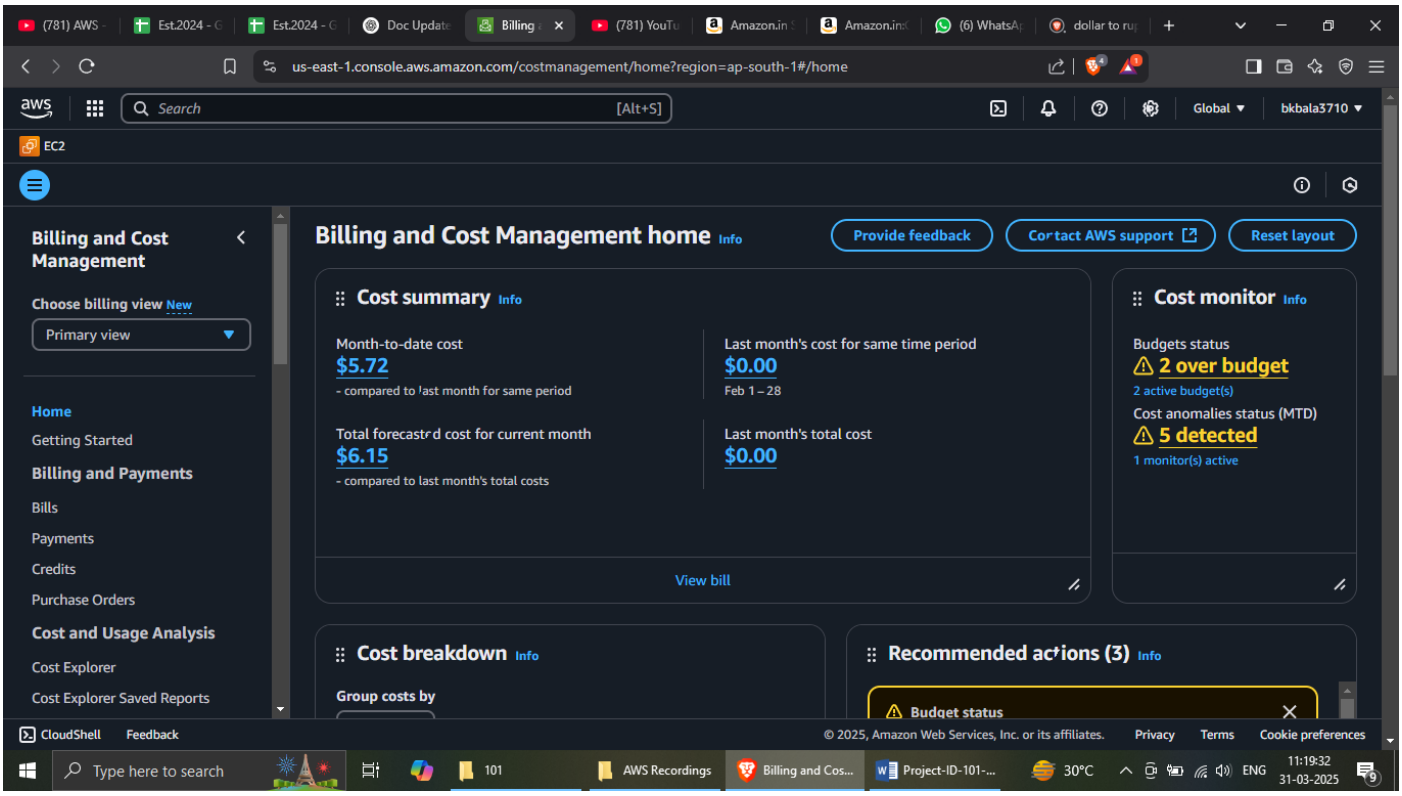


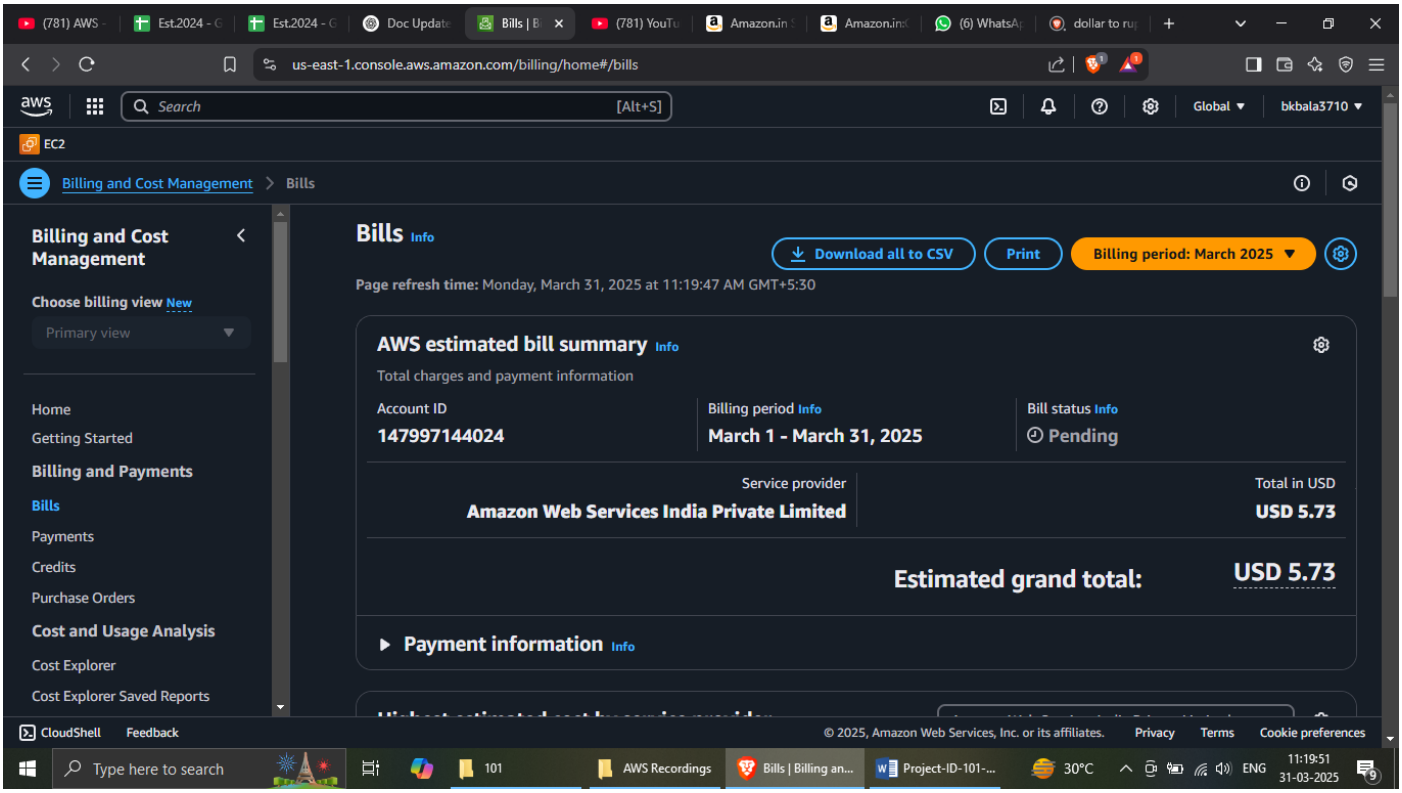


21.2 Auto scaling triggered SNS



22. Cost Management





Step to install web and app tier codes – configuration

1. Login to private-app-tier-ec2 instance via SSM system manager – connect (key not required – IAM)
2. sudo su (to became root user)
3. whoami (to ensure we are in root user)
4. cd . . (to move backward - /usr/bin to /usr)
5. pwd (to ensure we in /usr)
6. cd /home/ec2-user/ (to became to ec2-user)
7. pwd (to ensure we in /home/ec2-user)
8. ping 8.8.8.8 (to ensure internet access enabled via NAT)
9. sudo yum install mysql -y (ensure access to S3 amazon-linux-repos/*) – if endpoint gateway has bucket restrict policy.
10. mysql -h <DB EndPoint> -u admin -p
    Ex: mysql -h database-1.c380a08uukyc.ap-south-1.rds.amazonaws.com -u admin -p
11. Enter password
12. CREATE DATABASE webappdb;
13. SHOW DATABASES;
14. USE webappdb;
15. CREATE TABLE IF NOT EXISTS transactions(

    id INT NOT NULL AUTO_INCREMENT,

    amount DECIMAL(10,2),

    description VARCHAR(100),

    PRIMARY KEY(id)

```
);
```

16. SHOW TABLES;
17. INSERT INTO transactions (amount, description) VALUES ('400', 'groceries');
18. SELECT * FROM transactions;
19. exit
20. update the **application-code/app-tier/DbConfig.js** file with your database credentials.
21. curl -o- https://raw.githubusercontent.com/avizway1/aws_3tier_architecture/main/install.sh | bash
22. source ~/.bashrc
23. nvm install 16
24. nvm use 16 (You will see 'Now using node v16.20.2)
    Node Version Manager – nvm
25. npm install -g pm2 (You will see 'found 0 vulnerabilities)
26. cd ~/
27. sudo aws s3 cp s3://<S3BucketName>/application-code/app-tier/ app-tier –recursive
    Ex: sudo aws s3 cp s3://demo-3tier-project/application-code/app-tier/ app-tier –recursive
28. Ls (app-tier)
29. cd app-tier/
30. npm install
31. ls ----> You will see 'index.js' file. We have to start that.
32. pm2 start index.js (You will see the status as 'online')
33. To verify;

    pm2 list (or) pm2 status

    pm2 logs (You will not see anything in red colour, everything in white colour you should see)

    At the end you will see something like; http://localhost:4000

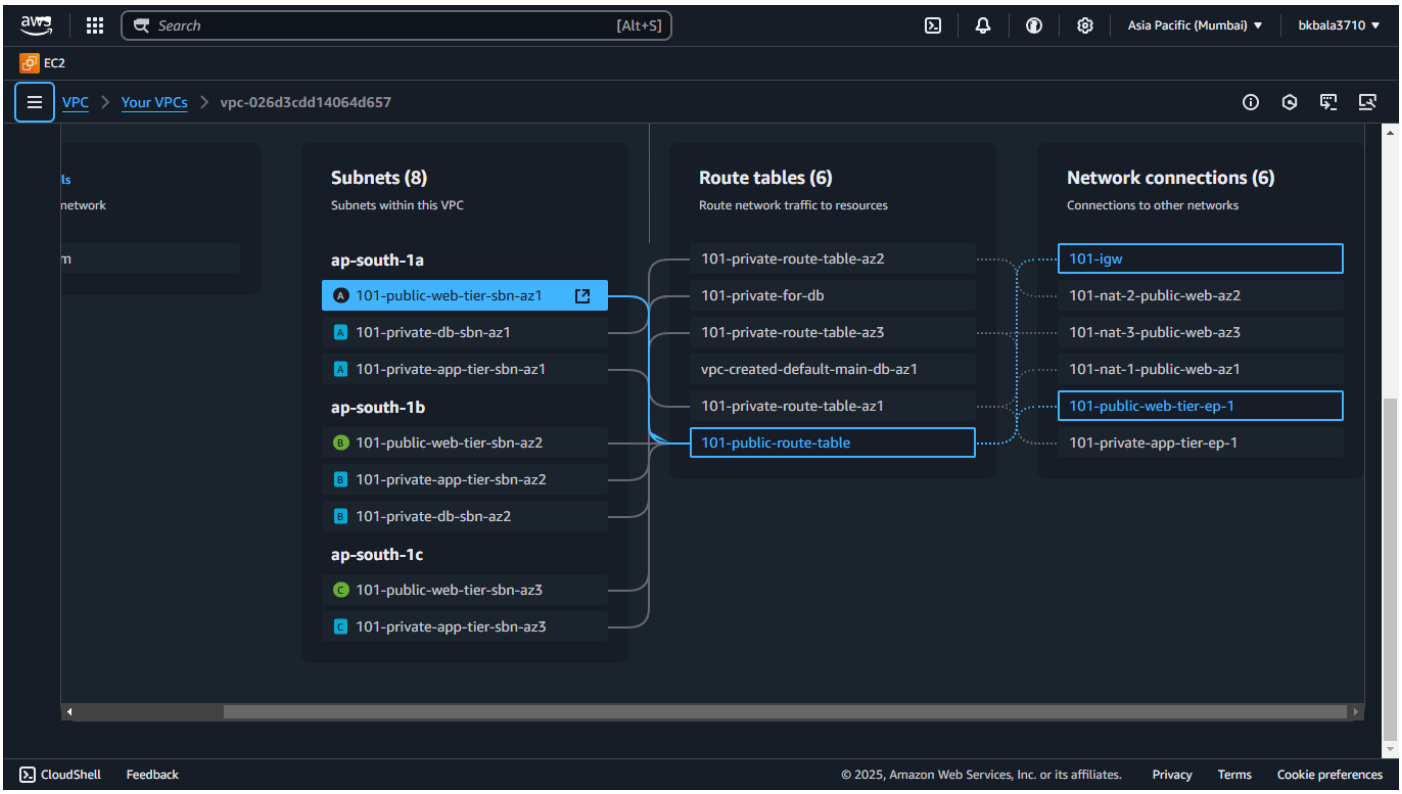
    ctrl + c – come out

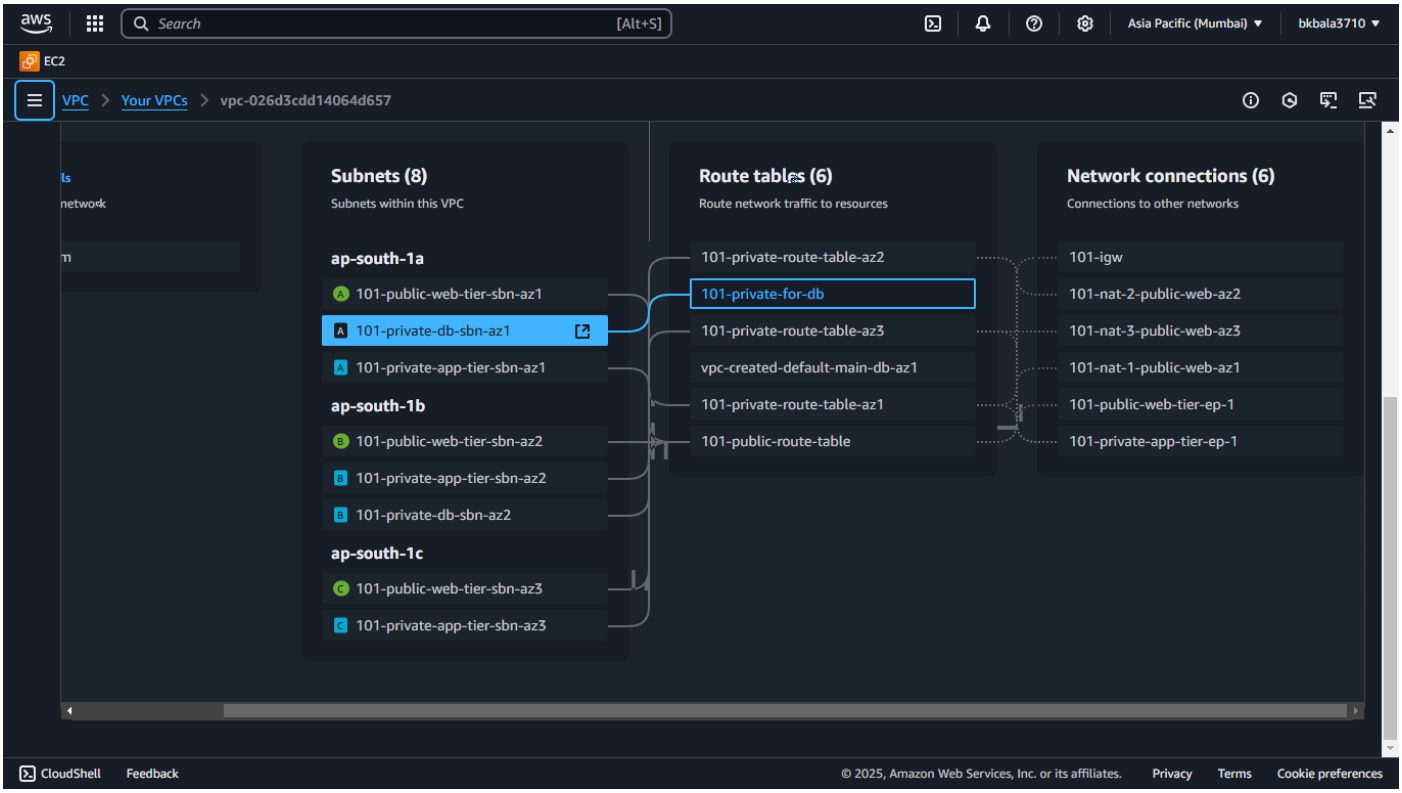
34. pm2 startup
35. pm2 save
36. curl http://localhost:4000/health

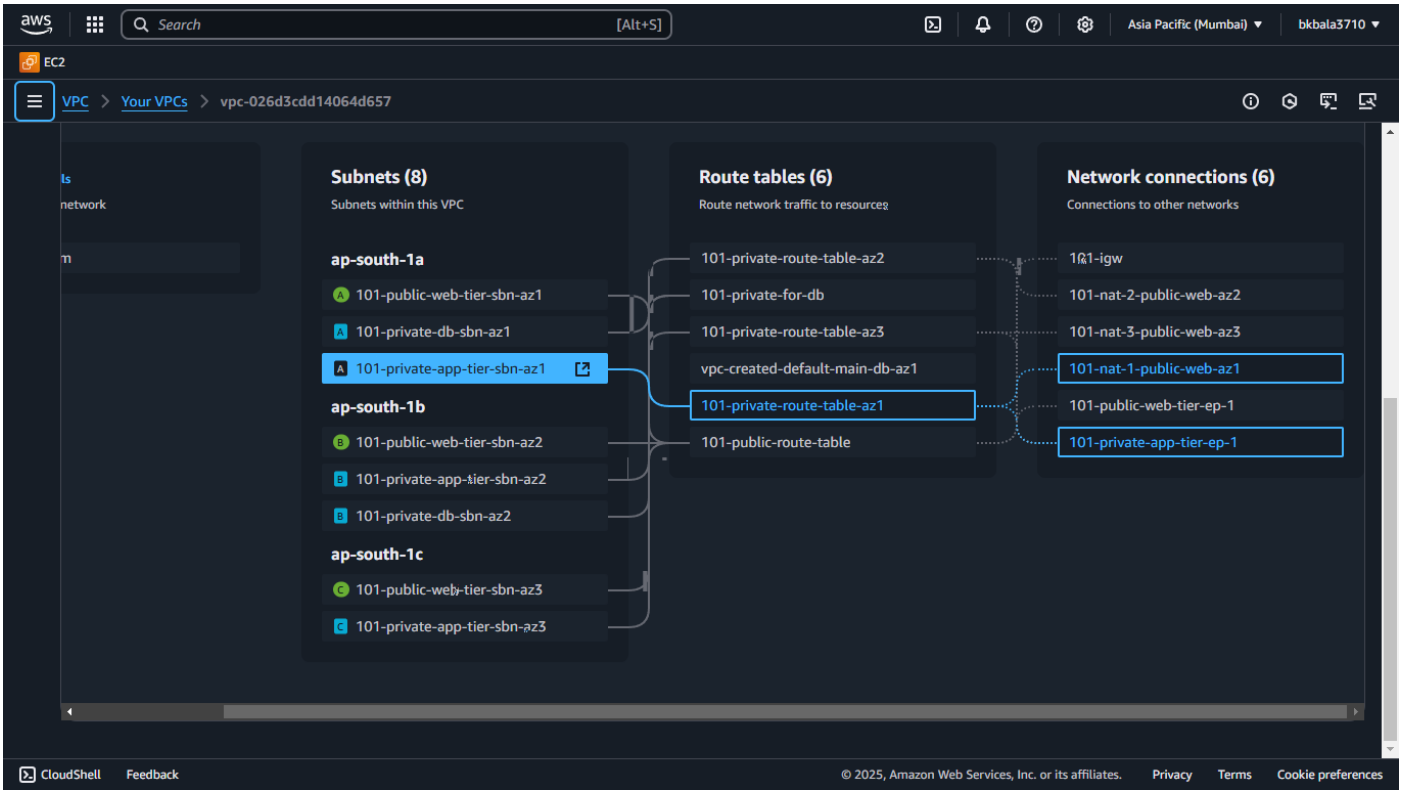
    It should return: This is the health check.

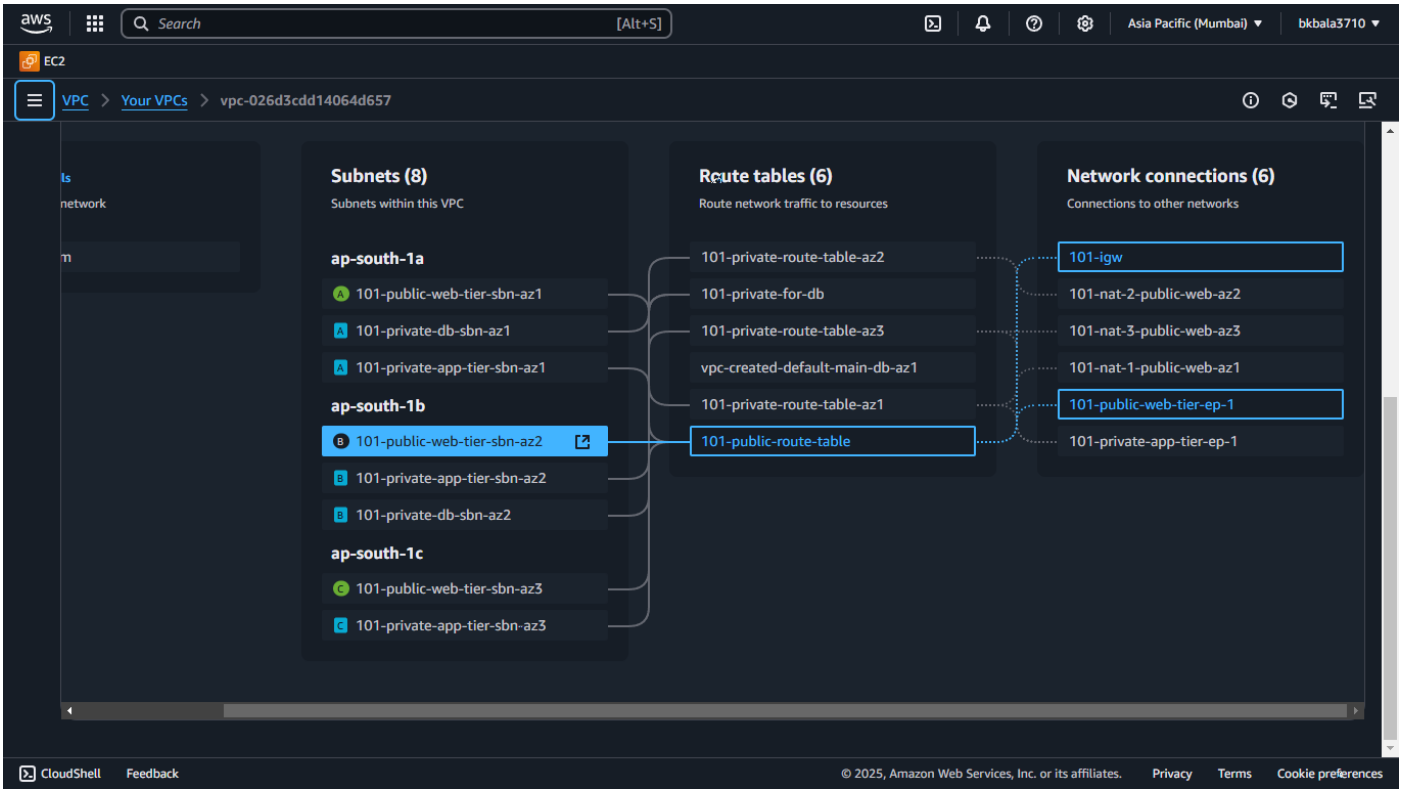
37. Creation of Internal Load Balancer for App Tier ec2 instance
38. Update the nginx.conf file in S3 with internal load balancer DNS.
39. Login to web tier ec2 via SSM system manager – connect (key not required – IAM)
40. sudo -su ec2-user
41. cd /home/ec2-user
42. curl -o- https://raw.githubusercontent.com/avizway1/aws_3tier_architecture/main/install.sh | bash
43. source ~/.bashrc
44. nvm install 16
45. nvm use 16
46. aws s3 cp s3://<S3 Bucker Name>/application-code/web-tier/ web-tier –recursive
    Ex: aws s3 cp s3://demo-3tier-project/application-code/web-tier/ web-tier –recursive
47. ls ----> You will see 'web-tier'

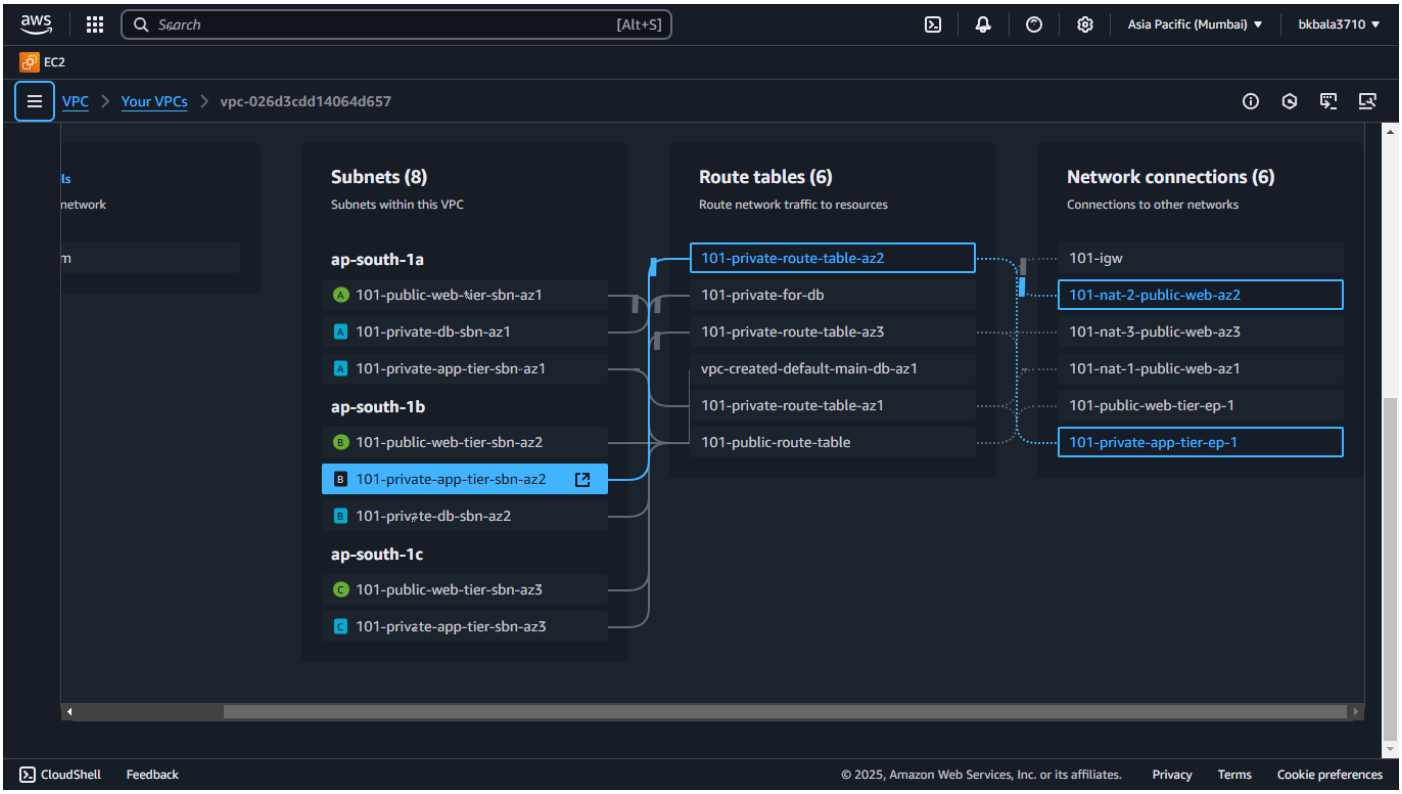
48. cd web-tier
49. npm install
50. npm run build
51. sudo amazon-linux-extras install nginx1 -y
52. cd /etc/nginx (Your are in nginx path)
53. ls ----> You will see 'nginx.conf' file
54. sudo rm nginx.conf
55. sudo aws s3 cp s3://<S3 Bucker Name>/application-code/nginx.conf .
    Ex: sudo aws s3 cp s3://demo-3tier-project/application-code/nginx.conf .
    (contains link to contact internal load balancer)
56. sudo service nginx restart
57. chmod -R 755 /home/ec2-user
58. sudo chkconfig nginx on
59. Browse the public IP of web tier ec2 if 0.0.0.0 enabled in SG – you can see the website running in 3 tier architecture.

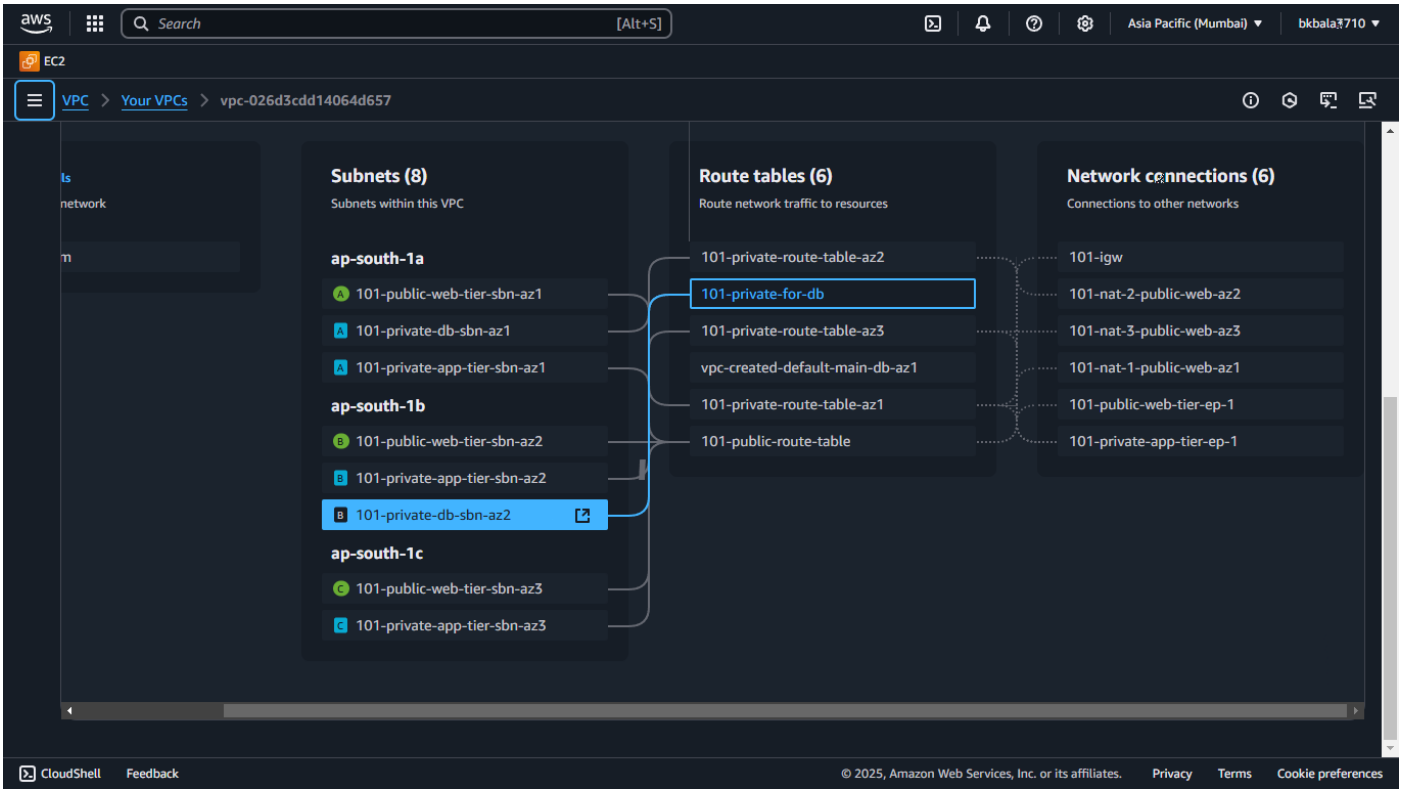


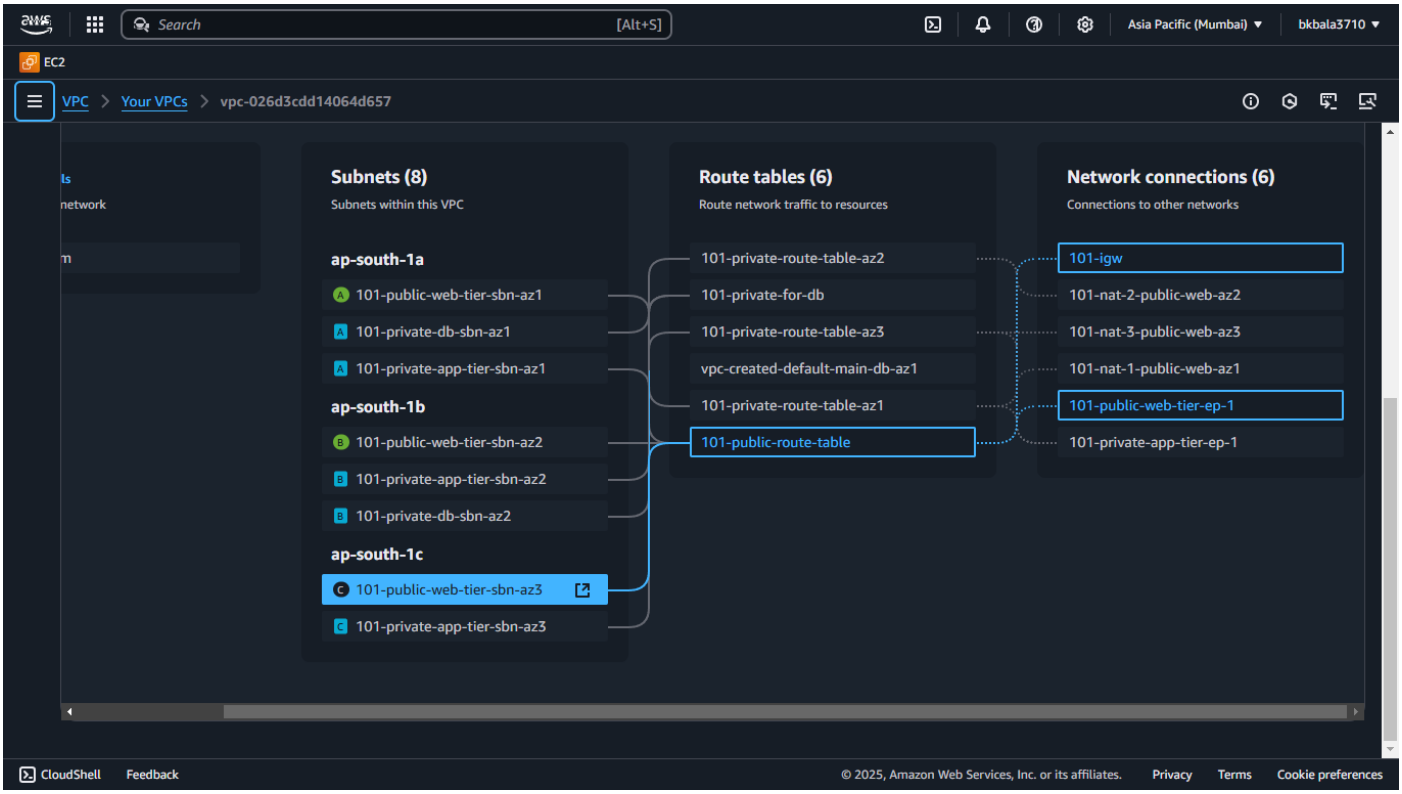

Search [Alt+S]
Asia Pacific (Mumbai)
bkbala3710
EC2
VPC > Your VPCs > vpc-026d3cdd14064d657
Subnets (8)
Subnets within this VPC
ap-south-1a
101-public-web-tier-sbn-az1
101-private-db-sbn-az1
101-private-app-tier-sbn-az1
ap-south-1b
101-public-web-tier-sbn-az2
101-private-app-tier-sbn-az2
101-private-db-sbn-az2
ap-south-1c
101-public-web-tier-sbn-az3
101-private-app-tier-sbn-az3
Route tables (6)
Route network traffic to resources
101-private-route-table-az2
101-private-for-db
101-private-route-table-az3
vpc-created-default-main-db-az1
101-private-route-table-az1
101-public-route-table
Network connections (6)
Connections to other networks
101-igw
101-nat-2-public-web-az2
101-nat-3-public-web-az3
101-nat-1-public-web-az1
101-public-web-tier-ep-1
101-private-app-tier-ep-1
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

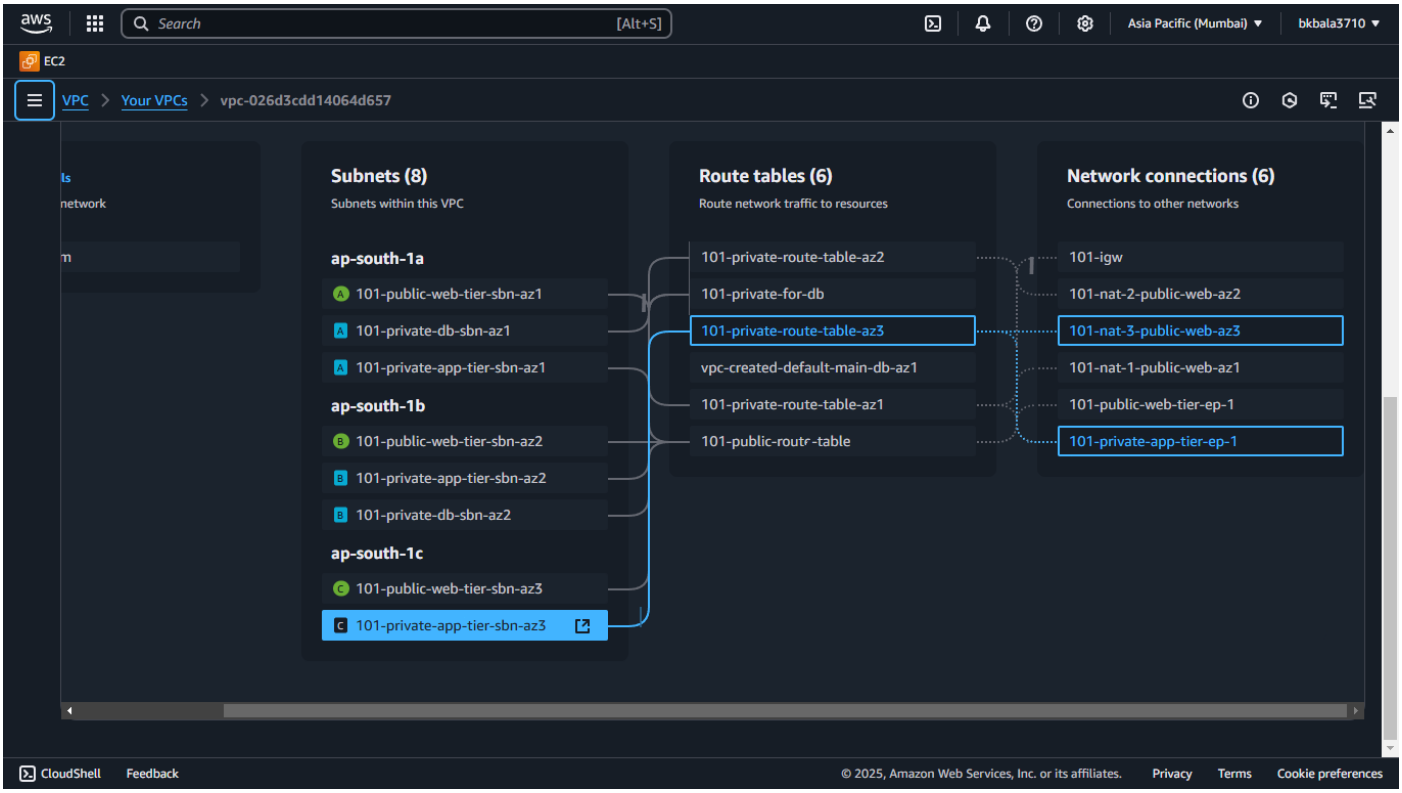

Search [Alt+S]
Asia Pacific (Mumbai)
bkbala3710
EC2
VPC > Your VPCs > vpc-026d3cdd14064d657
Subnets (8)
Subnets within this VPC
ap-south-1a
101-public-web-tier-sbn-az1
101-private-db-sbn-az1
101-private-app-tier-sbn-az1
ap-south-1b
101-public-web-tier-sbn-az2
101-private-app-tier-sbn-az2
101-private-db-sbn-az2
ap-south-1c
101-public-web-tier-sbn-az3
101-private-app-tier-sbn-az3
Route tables (6)
Route network traffic to resources
101-private-route-table-az2
101-private-for-db
101-private-route-table-az3
vpc-created-default-main-db-az1
101-private-route-table-az1
101-public-route-table
Network connections (6)
Connections to other networks
101-igw
101-nat-2-public-web-az2
101-nat-3-public-web-az3
101-nat-1-public-web-az1
101-public-web-tier-ep-1
101-private-app-tier-ep-1
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Asia Pacific (Mumbai)
bkbala3710
EC2
VPC > Your VPCs > vpc-026d3cdd14064d657
Subnets (8)
Subnets within this VPC
ap-south-1a
101-public-web-tier-sbn-az1
101-private-db-sbn-az1
101-private-app-tier-sbn-az1
ap-south-1b
101-public-web-tier-sbn-az2
101-private-app-tier-sbn-az2
101-private-db-sbn-az2
ap-south-1c
101-public-web-tier-sbn-az3
101-private-app-tier-sbn-az3
Route tables (6)
Route network traffic to resources
101-private-route-table-az2
101-private-for-db
101-private-route-table-az3
vpc-created-default-main-db-az1
101-private-route-table-az1
101-public-route-table
Network connections (6)
Connections to other networks
101-igw
101-nat-2-public-web-az2
101-nat-3-public-web-az3
101-nat-1-public-web-az1
101-public-web-tier-ep-1
101-private-app-tier-ep-1
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Asia Pacific (Mumbai)
bkbala3710
EC2
VPC > Your VPCs > vpc-026d3cdd14064d657
Subnets (8)
Subnets within this VPC
ap-south-1a
101-public-web-tier-sbn-az1
101-private-db-sbn-az1
101-private-app-tier-sbn-az1
ap-south-1b
101-public-web-tier-sbn-az2
101-private-app-tier-sbn-az2
101-private-db-sbn-az2
ap-south-1c
101-public-web-tier-sbn-az3
101-private-app-tier-sbn-az3
Route tables (6)
Route network traffic to resources
101-private-route-table-az2
101-private-for-db
101-private-route-table-az3
vpc-created-default-main-db-az1
101-private-route-table-az1
101-public-route-table
Network connections (6)
Connections to other networks
101-igw
101-nat-2-public-web-az2
101-nat-3-public-web-az3
101-nat-1-public-web-az1
101-public-web-tier-ep-1
101-private-app-tier-ep-1
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Asia Pacific (Mumbai)
bkbala3710
EC2
VPC > Your VPCs > vpc-026d3cdd14064d657
Subnets (8)
Subnets within this VPC
ap-south-1a
101-public-web-tier-sbn-az1
101-private-db-sbn-az1
101-private-app-tier-sbn-az1
ap-south-1b
101-public-web-tier-sbn-az2
101-private-app-tier-sbn-az2
101-private-db-sbn-az2
ap-south-1c
101-public-web-tier-sbn-az3
101-private-app-tier-sbn-az3
Route tables (6)
Route network traffic to resources
101-private-route-table-az2
101-private-for-db
101-private-route-table-az3
vpc-created-default-main-db-az1
101-private-route-table-az1
101-public-route-table
Network connections (6)
Connections to other networks
101-igw
101-nat-2-public-web-az2
101-nat-3-public-web-az3
101-nat-1-public-web-az1
101-public-web-tier-ep-1
101-private-app-tier-ep-1
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Search [Alt+S]
Asia Pacific (Mumbai)
bkbala3710
EC2
VPC > Your VPCs > vpc-026d3cdd14064d657
Subnets (8)
Subnets within this VPC
ap-south-1a
101-public-web-tier-sbn-az1
101-private-db-sbn-az1
101-private-app-tier-sbn-az1
ap-south-1b
101-public-web-tier-sbn-az2
101-private-app-tier-sbn-az2
101-private-db-sbn-az2
ap-south-1c
101-public-web-tier-sbn-az3
101-private-app-tier-sbn-az3
Route tables (6)
Route network traffic to resources
101-private-route-table-az2
101-private-for-db
101-private-route-table-az3
vpc-created-default-main-db-az1
101-private-route-table-az1
101-public-route-table
Network connections (6)
Connections to other networks
101-igw
101-nat-2-public-web-az2
101-nat-3-public-web-az3
101-nat-1-public-web-az1
101-public-web-tier-ep-1
101-private-app-tier-ep-1
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Note: I skipped route 53, cloud front, EFS, S3 event trigger – but we can also include those as described in architecture diagram for the excellent availability and functionality…
Will be updating the missed service in the upcoming days…

Reference link : https://www.youtube.com/watch?v=Oj-Hr_aulKA&t=721s