

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.

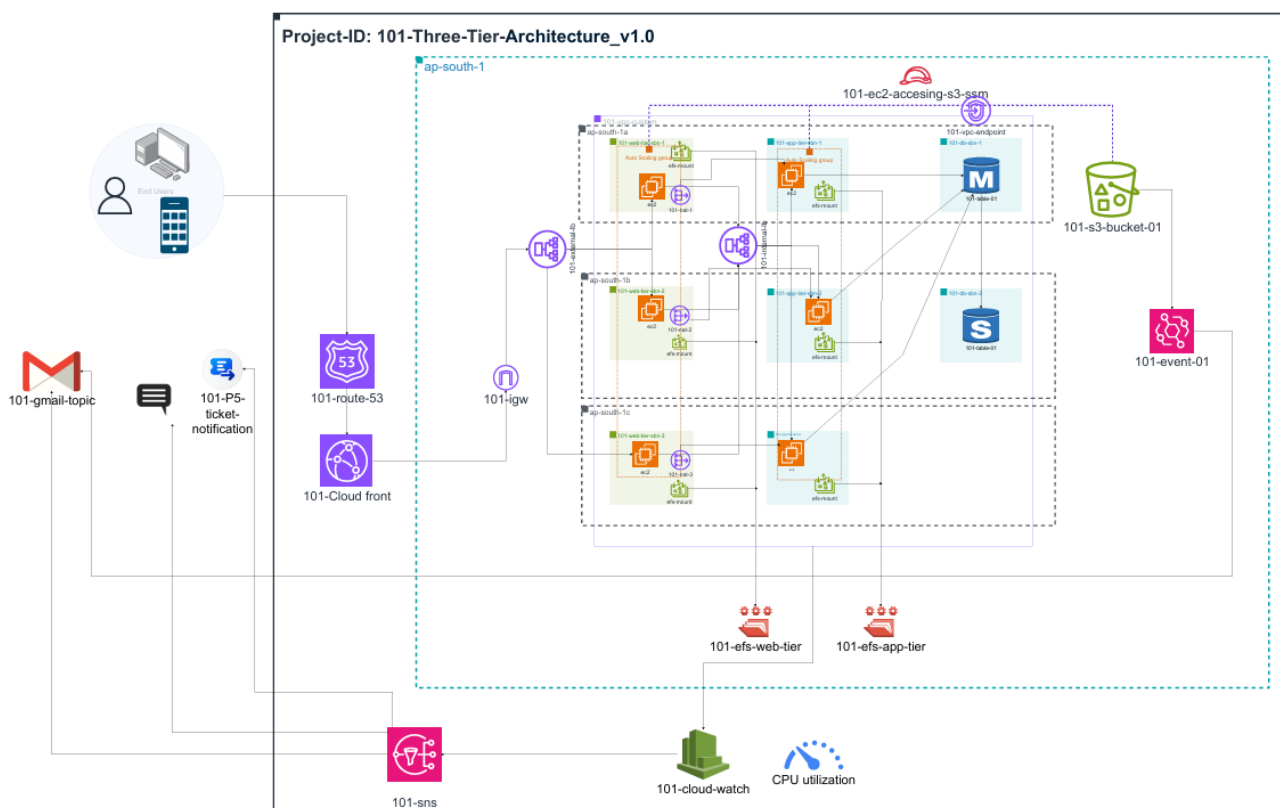
Architecture flow:

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

The screenshot shows the Amazon S3 console interface. The left sidebar contains navigation options for Amazon S3, including General purpose buckets, Directory buckets, Table buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, IAM Access Analyzer for S3, Storage Lens, Dashboards, and Storage Lens groups. The main content area is titled 'General purpose buckets (4)' and includes a search bar, a table of buckets, and buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'. The table lists four buckets, all in the Asia Pacific (Mumbai) region.

Name	AWS Region	IAM Access Analyzer	Creation date
101-app-tier-bucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	March 29, 2025, 11:38:44 (UTC+05:30)
101-s3-bucket-01	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	March 28, 2025, 21:45:21 (UTC+05:30)
101-web-tier-bucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	March 29, 2025, 11:38:19 (UTC+05:30)
102-feedback-collection-27-03-2025	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	March 27, 2025, 23:04:17 (UTC+05:30)

2. VPC – 101-vpc-custom

The screenshot shows the Amazon VPC console interface. The left sidebar contains navigation options for VPC dashboard, including Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, and NAT gateways. The main content area is titled 'Your VPCs (2)' and includes a search bar, a table of VPCs, and buttons for 'Actions' and 'Create VPC'. The table lists two VPCs, both in the 'Available' state.

Name	VPC ID	State	Block Public...	IPv4 CIDR
101-vpc-custom	vpc-026d3cdd14064d657	Available	Off	10.0.0.0/16
-	vpc-05225a81fd9b81e54	Available	Off	172.31.0.0/16

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

The screenshot shows the Amazon VPC console interface. The left sidebar contains navigation options for VPC dashboard, including Your VPCs, Subnets, Route tables, Internet gateways, Egress-only internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, and NAT gateways. The main content area is titled 'Subnets (8)' and includes a search bar, a table of subnets, and buttons for 'Actions' and 'Create subnet'. The table lists eight subnets, all in the 'Available' state.

Name	Subnet ID	State	VPC
101-private-app-tier-sbn-az2	subnet-0ac8791286e5ada0e	Available	vpc-026d3cdd14064d657 101-vpc-custom
101-public-web-tier-sbn-az1	subnet-031bffb9a851e7030	Available	vpc-026d3cdd14064d657 101-vpc-custom
101-private-db-sbn-az1	subnet-0229636ecb86c1e94	Available	vpc-026d3cdd14064d657 101-vpc-custom
101-public-web-tier-sbn-az3	subnet-04768f8a654a984b5	Available	vpc-026d3cdd14064d657 101-vpc-custom
101-private-db-sbn-az2	subnet-034fd96daa41fa476	Available	vpc-026d3cdd14064d657 101-vpc-custom
101-private-app-tier-sbn-az1	subnet-04b4a11e675f9a680	Available	vpc-026d3cdd14064d657 101-vpc-custom
101-private-app-tier-sbn-az3	subnet-072e850afc37bc6f7	Available	vpc-026d3cdd14064d657 101-vpc-custom
101-public-web-tier-sbn-az2	subnet-06222daac88d95a64	Available	vpc-026d3cdd14064d657 101-vpc-custom

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

Name	Route table ID	Explicit subnet associations
101-private-route-table-az2	rtb-09273bb3477243a20	subnet-0ac8791286e5ada0e / 101-private-app-tier-sbn-az2
101-private-for-db	rtb-06ad185397e934c78	2 subnets
101-private-route-table-az3	rtb-088f280234f36aed2	subnet-072e850afc37bc6f7 / 101-private-app-tier-sbn-az3
-	rtb-051a7296504684271	-
vpc-created-default-main-db-az1	rtb-03eb92087bcc9375b	-
101-private-route-table-az1	rtb-02f196a3f71fdc6b1	subnet-04b4a11e675f9a680 / 101-private-app-tier-sbn-az1
101-public-route-table	rtb-0c7eb77850db1492a	3 subnets

5. IGW-vpc

Name	Internet gateway ID	State	VPC ID
-	igw-05eb2a13515c0dc7a	Attached	vpc-05225a81fd9b81e54
101-igw	igw-0b85e7805a1773001	Attached	vpc-026d3cdd14064d657 / 101-vpc-cu...

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

Name	Allocated IPv4 address	Type	Allocation ID	Reverse DNS
-	13.202.202.255	Public IP	eipalloc-09fdd73e17c76db81	-
-	13.202.53.198	Public IP	eipalloc-0726b73d240ee8271	-
-	35.154.113.169	Public IP	eipalloc-0647804089cc7a96b	-

7. 3NAT in 3az public

Name	NAT gateway ID	Connectivity...	State	State message	Primary
101-nat-3-public-web-az3	nat-0813175a15a3c2f69	Public	Available	-	13.202
101-nat-1-public-web-az1	nat-08d74c56eaeab3318	Public	Available	-	13.202
101-nat-2-public-web-az2	nat-05a7cce02f722b86a	Public	Available	-	35.154

8. NACLs - 1 - VPC

Name	Network ACL ID	Associated with	Default	VPC ID
-	acl-0eae6c3c47f3f2af	3 Subnets	Yes	vpc-05225a81fd9b81e54
-	acl-0800dbde68a4661e5	8 Subnets	Yes	vpc-026d3cdd14064d657 /

8.1. NACLs - inbound

The screenshot shows the AWS IAM console interface for a Network ACL. The left sidebar contains navigation links for Virtual private cloud, Security, and PrivateLink and. The main content area displays details for the Network ACL **acl-0800dbde68a4661e5**. The **Inbound rules** tab is selected, showing a table with 2 rules. The first rule (100) allows all traffic from 0.0.0.0/0. The second rule (*) denies all traffic from 0.0.0.0/0.

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

8.2. NACLs - Outbound

The screenshot shows the AWS IAM console interface for a Network ACL. The left sidebar contains navigation links for Virtual private cloud, Security, and PrivateLink and. The main content area displays details for the Network ACL **acl-0800dbde68a4661e5**. The **Outbound rules** tab is selected, showing a table with 2 rules. The first rule (100) allows all traffic to 0.0.0.0/0. The second rule (*) denies all traffic to 0.0.0.0/0.

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

9. Security groups - 5

The screenshot shows the AWS IAM console interface for Security Groups. The left sidebar contains navigation links for Virtual private cloud, Security, and PrivateLink and. The main content area displays a list of 7 Security Groups. The table shows the Name, Security group ID, Security group name, and VPC ID for each group.

Name	Security group ID	Security group name	VPC ID
-	sg-0792bff3d1e7df965	default	vpc-05225a81fd9b81e54
101-private-app-sg	sg-0e839d795c1cfeeab	101-private-app-sg	vpc-026d3cdd14064d6f7
-	sg-07942972c8cb62d5c	default	vpc-026d3cdd14064d657
101-private-db-sg	sg-0ba43aea5d1eef9b0	101-private-db-sg	vpc-026d3cdd14064d657
101-external-lb-sg	sg-0c2afcac5639d415	101-external-lb-sg	vpc-026d3cdd14064d657
101-public-web-sg	sg-052bfaf44e66e7520	101-public-web-sg	vpc-026d3cdd14064d657
101-internal-lb-sg	sg-08b9c9fcd9bb43933	101-internal-lb-sg	vpc-026d3cdd14064d657

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

sg-0c2afcacc5639d415 - 101-external-lb-sg Actions

Details

Security group name 101-external-lb-sg	Security group ID sg-0c2afcacc5639d415	Description http-access	VPC ID vpc-026d3cdd14064d657
Owner 147997144024	Inbound rules count 1 Permission entry	Outbound rules count 2 Permission entries	

Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

Inbound rules (1) Manage tags Edit inbound rules

Search

Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
sgr-01fd4afdb7c7cc127	IPv4	HTTP	TCP	80	0.0.0.0/0	-

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

sg-052bfaf44e66e7520 - 101-public-web-sg Actions

Details

Security group name 101-public-web-sg	Security group ID sg-052bfaf44e66e7520	Description http only from external lb	VPC ID vpc-026d3cdd14064d657
Owner 147997144024	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

Inbound rules (2) Manage tags Edit inbound rules

Search

Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
sgr-0531e494d9f794f8c	-	HTTP	TCP	80	sg-0c2afcacc5639d415 ...	-

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

sg-08b9c9fcd9bb43933 - 101-internal-lb-sg Actions

Details

Security group name 101-internal-lb-sg	Security group ID sg-08b9c9fcd9bb43933	Description http only from public web tier	VPC ID vpc-026d3cdd14064d657
Owner 147997144024	Inbound rules count 1 Permission entry	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

Inbound rules (1) Manage tags Edit inbound rules

Search

Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
sgr-04a0d316a310178ae	-	HTTP	TCP	80	sg-052bfaf44e66e7520...	-

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

sg-0e839d795c1cfeeab - 101-private-app-sg Actions

Details

Security group name 101-private-app-sg	Security group ID sg-0e839d795c1cfeeab	Description http only from internal lb	VPC ID vpc-026d3cdd14064d657
Owner 147997144024	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

Inbound rules (2) Manage tags Edit inbound rules

Search

Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
sgr-03a48e2d32b131650	-	Custom TCP	TCP	4000	sg-08b9c9fcd9bb43933...	-

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

sg-0ba43aea5d1eef9b0 - 101-private-db-sg

Details

Security group name

101-private-db-sg

Security group ID

sg-0ba43aea5d1eef9b0

Description

only from private subnet

VPC ID

vpc-026d3cdd14064d657

Owner

147997144024

Inbound rules count

1 Permission entry

Outbound rules count

1 Permission entry

Inbound rules

Outbound rules

Sharing - new

VPC associations - new

Tags

Inbound rules (1)

Search

Manage tags

Edit inbound rules

Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
sgr-02cdebc0cd21cc449	-	MYSQL/Aurora	TCP	3306	sg-0e839d795c1cfeeab...	-

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

Endpoints (2)

Search

Actions

Create endpoint

Name	VPC endpoint ID	Endpoint type	Status
101-public-web-tier-ep-1	vpce-0c00f1ddec60abf92	Gateway	Available
101-private-app-tier-ep-1	vpce-00e3d8fb86430d134	Gateway	Available

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

vpce-0c00f1ddec60abf92 / 101-public-web-tier-ep-1

Details

Endpoint ID

vpce-0c00f1ddec60abf92

Status

Available

Creation time

Saturday, March 29, 2025 at 19:16:39 GMT+5:30

Endpoint type

Gateway

VPC ID

vpc-026d3cdd14064d657 (101-vpc-custom)

Status message

-

Service name

com.amazonaws.ap-south-1.s3

Private DNS names enabled

No

Route tables

Policy

Tags

Route tables (1)

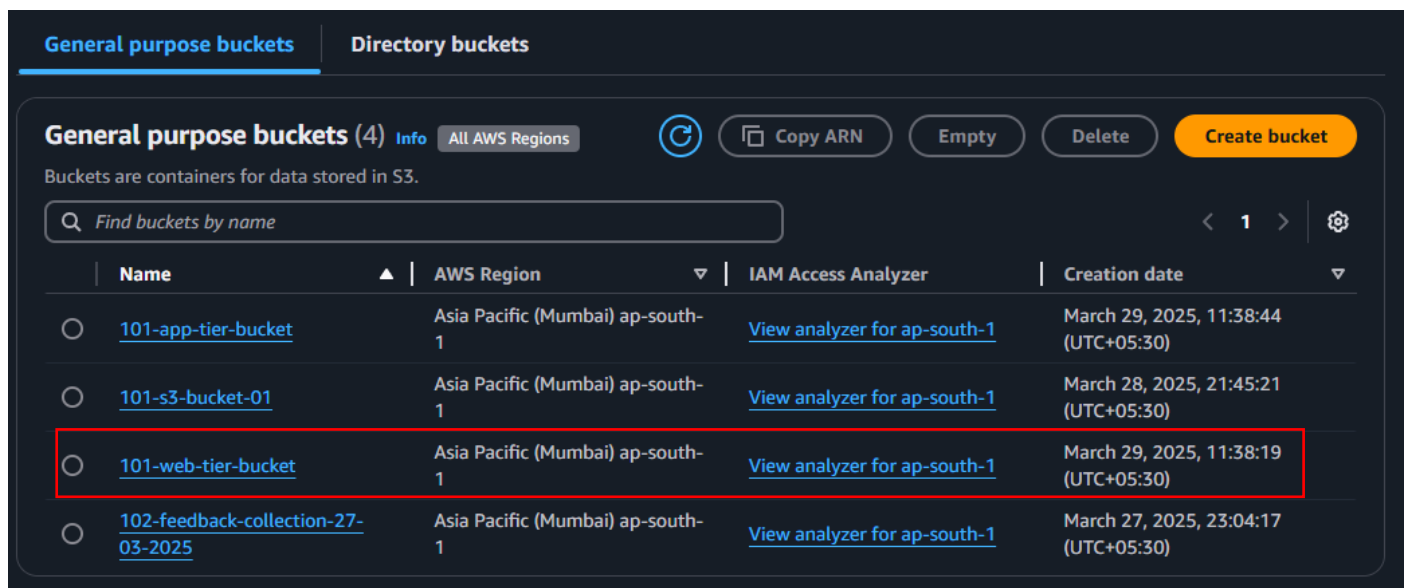
Search

Manage route tables

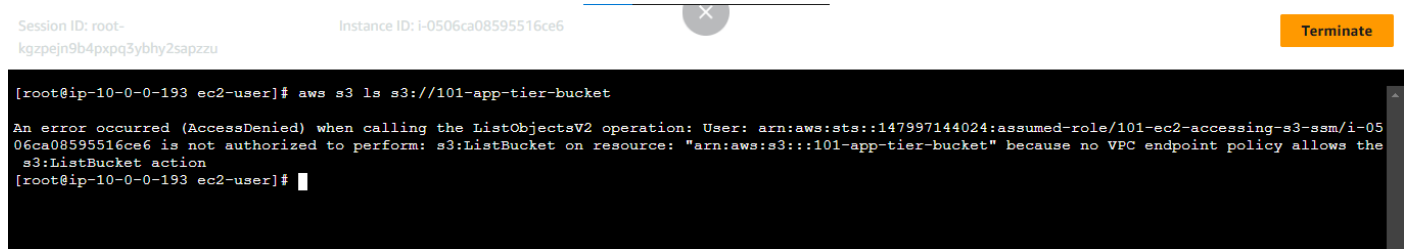
Name	Route Table ID	Main
101-public-route-table	rtb-0c7eb77850db1492a (101-public-route-table)	No

7

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

vpce-00e3d8fb86430d134 / 101-private-app-tier-ep-1 Actions

Details

Endpoint ID
vpce-00e3d8fb86430d134

VPC ID
vpc-026d3cdd14064d657 (101-vpc-custom)

Status
Available

Status message
–

Creation time
Saturday, March 29, 2025 at 19:18:46 GMT+5:30

Service name
com.amazonaws.ap-south-1.s3

Endpoint type
Gateway

Private DNS names enabled
No

Route tables

Policy

Tags

Route tables (3) Manage route tables

Name	Route Table ID	Main
101-private-route-table-az2	rtb-09273bb3477243a20 (101-private-route-table-az2)	No
101-private-route-table-az3	rtb-088f280234f36aed2 (101-private-route-table-az3)	No
101-private-route-table-az1	rtb-02f196a3f71fdc6b1 (101-private-route-table-az1)	No

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

VPC endpoint policy controls access to the service

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Principal": "*",
7       "Action": "s3:*",
8       "Resource": [
9         "arn:aws:s3:::101-app-tier-bucket",
10        "arn:aws:s3:::101-app-tier-bucket/*"
11      ]
12    }
13  ]
14 }
```

General purpose buckets

Directory buckets

General purpose buckets (4) Info All AWS Regions

Refresh

Copy ARN

Empty

Delete

Create bucket

Buckets are containers for data stored in S3.

Find buckets by name

< 1 > ⚙

	Name	AWS Region	IAM Access Analyzer	Creation date
<input type="radio"/>	101-app-tier-bucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	March 29, 2025, 11:38:44 (UTC+05:30)
<input type="radio"/>	101-s3-bucket-01	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	March 28, 2025, 21:45:21 (UTC+05:30)
<input type="radio"/>	101-web-tier-bucket	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	March 29, 2025, 11:38:19 (UTC+05:30)
<input type="radio"/>	102-feedback-collection-27-03-2025	Asia Pacific (Mumbai) ap-south-1	View analyzer for ap-south-1	March 27, 2025, 23:04:17 (UTC+05:30)

only can view app tier bucket as mentioned in policy

Session ID: root-5abfyxivubs9og9eq4x46v7py

Instance ID: i-0048b0f7178eedc49

Terminate

✕

```
[root@ip-10-0-3-92 bin]# aws s3 ls
2025-03-29 06:08:44 101-app-tier-bucket
2025-03-28 16:15:21 101-s3-bucket-01
2025-03-29 06:08:19 101-web-tier-bucket
2025-03-27 17:34:17 102-feedback-collection-27-03-2025
[root@ip-10-0-3-92 bin]# aws s3 ls s3://101-s3-bucket-01/

An error occurred (AccessDenied) when calling the ListObjectsV2 operation: User: arn:aws:sts::147997144024:assumed-role/101-ec2-accessing-s3-ssm/i-0048b0f7178eedc49 is not authorized to perform: s3:ListBucket on resource: "arn:aws:s3:::101-s3-bucket-01" because no VPC endpoint policy allows the s3:ListBucket action
[root@ip-10-0-3-92 bin]# aws s3 ls s3://101-app-tier-bucket
[root@ip-10-0-3-92 bin]#
```

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

Auto Scaling groups (2) Info

Launch configurations

Launch templates

Actions

Create Auto Scaling group

Search your Auto Scaling groups

< 1 > ⚙

<input type="checkbox"/>	Name	Launch template/configuration	Instances	Status	Desired capacity
<input type="checkbox"/>	101-private-web-tier-as	101-private-app-tier-template Version C	1	-	1
<input type="checkbox"/>	101-public-web-tier-as	101-public-web-tier-template Version D	1	-	1

11.1 Public-web-tier

101-public-web-tier-as

101-public-web-tier-as Capacity overview

am:aws:autoscaling:ap-south-1:147997144024:autoScalingGroup:7e17ba31-f2c4-4901-b872-31ddd53f1799:autoScalingGroupName/101-public-web-tier-as

Desired capacity	Scaling limits (Min - Max)	Desired capacity type	Status
1	1 - 2	Units (number of instances)	-

Date created

Sat Mar 29 2025 19:08:44 GMT+0530 (India Standard Time)

Edit

<

Details

Integrations - new

Automatic scaling

Instance management

Instance refresh

Activity

>

Launch template

Launch template

lt-0a3e36a68d23cae76

101-public-web-tier-template

AMI ID

ami-04eed0e618979ba41

Instance type

t2.micro

Owner

arn:aws:iam::147997144024:root

Version

Default

Security groups

-

Security group IDs

sg-052bfaf44e66e7520

Create time

Sat Mar 29 2025 19:05:05 GMT+0530 (India Standard Time)

Edit

*Launch template

Launch Templates (2) Info

Actions

Create launch template

Search

<input type="checkbox"/>	Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time
<input type="checkbox"/>	lt-045ddec48d7896ee5	101-private-app-tier-template	1	1	2025-03-29T13:36:55.000Z
<input type="checkbox"/>	lt-0a3e36a68d23cae76	101-public-web-tier-template	1	1	2025-03-29T13:35:05.000Z

101-publr-web-tier-template (lt-0a3e36a68d23cae76)

ActionsDelete 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

ActionsDelete 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-Scalingr-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)

101-private-web-tier-as

101-private-web-tier-as Capacity overview

arn:aws:autoscaling:ap-south-1:147997144024:autoScalingGroup:3f6d9f53-8f91-4efb-bba8-d3ebf6815ed9:autoScalingGroupName/101-private-web-tier-as

Desired capacity	Scaling limits (Min - Max)	Desired capacity type	Status
1	1 - 2	Units (number of instances)	-

Date created
Sat Mar 29 2025 19:10:16 GMT+0530 (India Standard Time)

Details

Integrations - new

Automatic scaling

Instance management

Instance refresh

Activity

Launch template

Launch template

lt-045ddec48d7896ee5

101-private-app-tier-template

AMI ID

ami-0c373e3995666b7bb

Instance type

t2.micro

Owner

arn:aws:iam::147997144024:root

Version

Default

Security groups

-

Security group IDs

sg-0e839d795c1cfeeab

Create time

Sat Mar 29 2025 19:06:55 GMT+0530 (India Standard Time)

*Launch template

Launch Templates (2)

Search

Actions

Create launch template

	Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time
<input type="checkbox"/>	lt-045ddec48d7896ee5	101-private-app-tier-template	1	1	2025-03-29T13:36:55.000Z
<input type="checkbox"/>	lt-0a3e36a68d23cae76	101-public-web-tier-template	1	1	2025-03-29T13:35:05.000Z

13

101-private-app-tier-template (lt-045ddec48d7896ee5)

Actions ▼Delete template

Launch template details

Launch template ID lt-045ddec48d7896ee5	Launch template name 101-private-app-tier-template	Default version 1	Owner arn:aws:iam::147997144024:root
--	---	----------------------	---

DetailsVersionsTemplate 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 detailsStorageResource tagsNetwork interfacesAdvanced 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

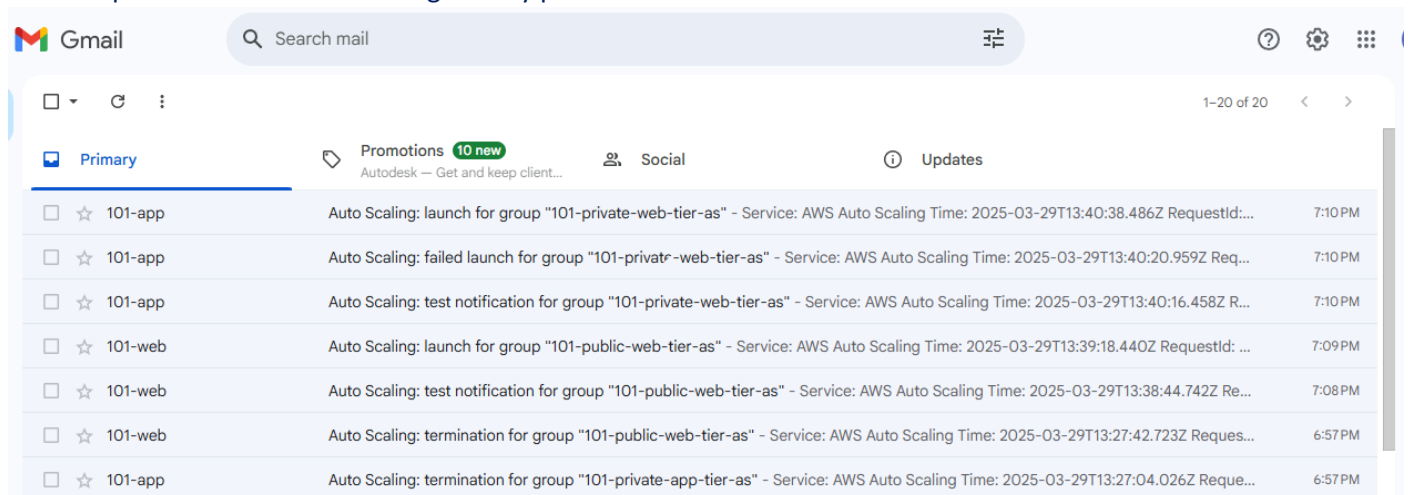
Take the action

Add 1 capacity units

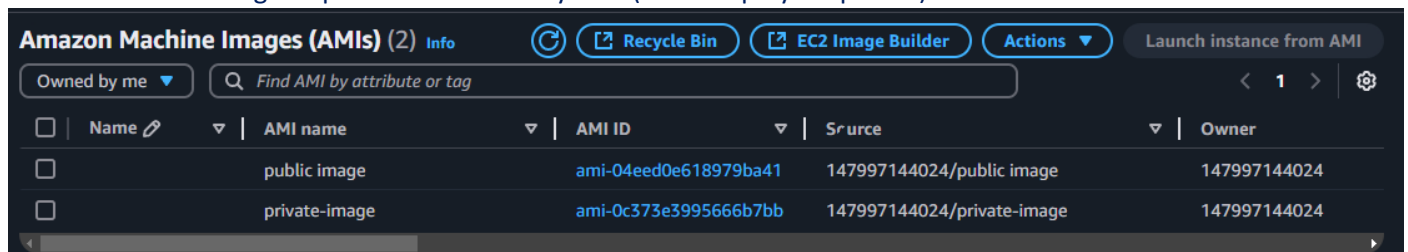
And then wait

300 seconds before allowing another scaling activity

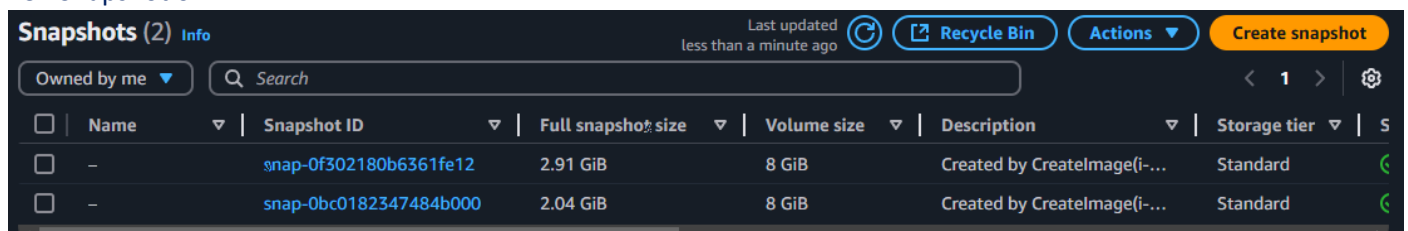
SNS – Topic enabled for each scaling activity performed.



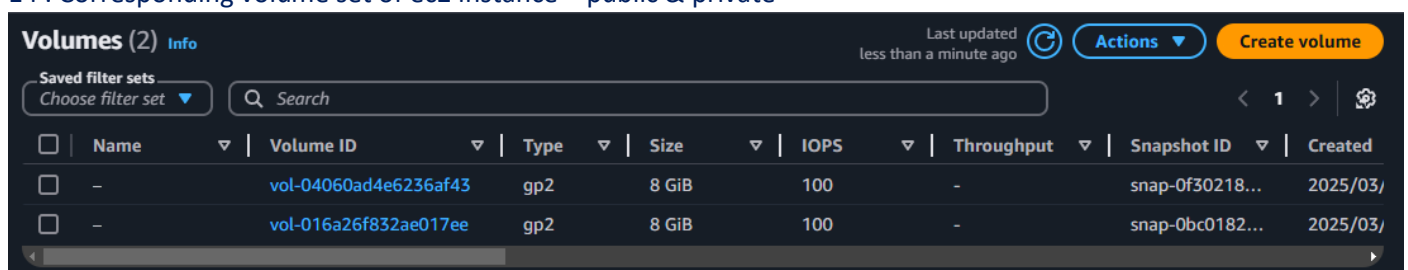
12. AMI – Autoscaling template was created by AMI (backedup by snapshots)



13 . Snapshot of AMI



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



15. LB – internal & external

Load balancers (2) Actions Create load balancer

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Filter load balancers

<input type="checkbox"/>	Name	DNS name	State	VPC ID	Availability
<input type="checkbox"/>	101-internal-lb-1	internal-101-internal-lb-1-548481610.ap-south-1.elb.a...	Active	vpc-026d3cdd14064d657	3 Availability
<input type="checkbox"/>	101-external-lb-1	101-external-lb-1-182610859.ap-south-1.elb.amazona...	Active	vpc-026d3cdd14064d657	3 Availability

15.1 LB corresponding target groups

Target groups (2) Actions Create target group

Filter target groups

<input type="checkbox"/>	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
<input type="checkbox"/>	101-external-lb-tg-1	arn:aws:elasticloadbalancing:ap-south-1:147997144024:targetgroup/101-external-lb-tg-1/200359a2bdd784c1	80	HTTP	Instance	101-external-lb-1	vpc-026d3cdd14064d657
<input type="checkbox"/>	101-internal-lb-tg-1	arn:aws:elasticloadbalancing:ap-south-1:147997144024:targetgroup/101-internal-lb-tg-1/49ef455577ee5c6f	4000	HTTP	Instance	101-internal-lb-1	vpc-026d3cdd14064d657

101-external-lb-tg-1 Actions

Details
arn:aws:elasticloadbalancing:ap-south-1:147997144024:targetgroup/101-external-lb-tg-1/200359a2bdd784c1

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC vpc-026d3cdd14064d657
IP address type IPv4	Load balancer 101-external-lb-1		

1 Total targets	1 Healthy	0 Unhealthy	0 Unused	0 Initial	0 Draining
	0 Anomalous				

101-internal-lb-tg-1 Actions

Details
arn:aws:elasticloadbalancing:ap-south-1:147997144024:targetgroup/101-internal-lb-tg-1/49ef455577ee5c6f

Target type Instance	Protocol : Port HTTP: 4000	Protocol version HTTP1	VPC vpc-026d3cdd14064d657
IP address type IPv4	Load balancer 101-internal-lb-1		

1 Total targets	1 Healthy	0 Unhealthy	0 Unused	0 Initial	0 Draining
	0 Anomalous				

16. RDS database

Databases (1) Group resources Modify Actions Restore from S3 Create database

Filter by databases

DB identifier	Status	Role	Engine	Region	Size
database-1	Available	Instance	MySQL Co...	ap-south-1a	db.t4g.micro

sbnggrp01-101

Subnet group details

VPC ID
vpc-026d3cdd14064d657

ARN
arn:aws:rds:ap-south-1:147997144024:subgrp:sbnggrp01-101

Supported network types
IPv4

Description
sbnggrp01-101

Subnets (2)

Availability zone	Subnet name	Subnet ID	CIDR block
ap-south-1a	101-private-db-sbn-az1	subnet-0229636ecb86c1e94	10.0.6.0/24
ap-south-1b	101-private-db-sbn-az2	subnet-034fd96daa41fa476	10.0.7.0/24

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)

rtb-0c7eb77850db1492a / 101-public-route-table Actions

Details Info

Route table ID
[rtb-0c7eb77850db1492a](#)

VPC
vpc-026d3cdd14064d657 | 101-vpc-custom

Main
No

Owner ID
[147997144024](#)

Explicit subnet associations
[3 subnets](#)

Edge associations
-

Routes Subnet associations Edge associations Route propagation Tags

Routes (3) Both Edit routes


Filter routes

Destination	Target	Status	Propagated
pl-78a54011	vpce-0c00f1ddec60abf92	Active	No
0.0.0.0/0	igw-0b85e7805a1773001	Active	No
10.0.0.0/16	local	Active	No


No subnet association just created when the VPC created


rtb-03eb92087bcc9375b / vpc-created-default-main-db-az1 Actions

Details Info

Route table ID
 rtb-03eb92087bcc9375b

VPC
vpc-026d3cdd14064d657 | 101-vpc-custom

Main
 Yes

Owner ID
 147997144024

Explicit subnet associations
–

Edge associations
–

Routes

Subnet associations

Edge associations

Route propagation

Tags


Routes (1) Both Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No


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


rtb-02f196a3f71fdc6b1 / 101-private-route-table-az1 Actions

Details Info

Route table ID
 rtb-02f196a3f71fdc6b1

VPC
vpc-026d3cdd14064d657 | 101-vpc-custom

Main
 No

Owner ID
 147997144024

Explicit subnet associations
subnet-04b4a11e675f9a680 / 101-private-app-tier-sbn-az1

Edge associations
–

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (3) Both Edit routes

Destination	Target	Status	Propagated
pl-78a54011	vpce-00e3d8fb86430d134	Active	No
0.0.0.0/0	nat-08d74c56eaeab3318	Active	No
10.0.0.0/16	local	Active	No

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

rtb-09273bb3477243a20 / 101-private-route-table-az2 Actions ▾

Details Info

Route table ID
rtb-09273bb3477243a20

VPC
vpc-026d3cdd14064d657 | 101-vpc-custom

Main
No

Owner ID
147997144024

Explicit subnet associations
subnet-0ac8791286e5ada0e / 101-private-app-tier-sbn-az2

Edge associations
–

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (3) Both ▾ Edit routes

Destination ▾

Target ▾

Status ▾

Propagated ▾

pl-78a54011	vpce-00e3d8fb86430d134	✓ Active	No
0.0.0.0/0	nat-05a7cce02f722b86a	✓ Active	No
10.0.0.0/16	local	✓ Active	No

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

rtb-088f280234f36aed2 / 101-private-route-table-az3 Actions ▾

Details Info

Route table ID
rtb-088f280234f36aed2

VPC
vpc-026d3cdd14064d657 | 101-vpc-custom

Main
No

Owner ID
147997144024

Explicit subnet associations
subnet-072e850afc37bc6f7 / 101-private-app-tier-sbn-az3

Edge associations
–

Routes

Subnet associations

Edge associations

Route propagation

Tags

Routes (3) Both ▾ Edit routes

Destination ▾

Target ▾

Status ▾

Propagated ▾

pl-78a54011	vpce-00e3d8fb86430d134	✓ Active	No
0.0.0.0/0	nat-0813175a15a3c2f69	✓ Active	No
10.0.0.0/16	local	✓ Active	No

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

rtb-06ad185397e934c78 / 101-private-for-db

Details Info

Route table ID
rtb-06ad185397e934c78

VPC
vpc-026d3cdd14064d657 | 101-vpc-custom

Main
No

Owner ID
147997144024

Explicit subnet associations
2 subnets

Edge associations
–

Routes Subnet associations Edge associations Route propagation Tags

Routes (1) Both Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

18. Topic & subscriptions

Amazon SNS > Topics

Amazon SNS < Topics (2) Edit Delete Publish message Create topic

Name	Type	ARN
101-private-app-tier	Standard	arn:aws:sns:ap-south-1:147997144024:101...
101-public-web-tier	Standard	arn:aws:sns:ap-south-1:147997144024:101...

19. Cloud watch alarm with SNS enabled -

Alarms (2)

☐ Hide Auto Scaling alarms Clear selection Create composite alarm Actions Create alarm

Alarm state: Insufficient ... Alarm type: Any Actions status: Any

Name	State	Last state update (UTC)	Conditions	Actions
101-private-app-tier-alarm	Insufficient data	2025-03-29 13:54:00	CPUUtilization >= 50 for 1 datapoints within 5 minutes	Actions enabled
101-public-web-tier-alarm	Insufficient data	2025-03-29 13:52:27	CPUUtilization >= 50 for 1 datapoints within 5 minutes	Actions enabled

19.1 Alarm triggered SNS

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

101-web

<no-reply@sns.amazonaws.com>

to me

12:03 AM (8 hours ago)

☆

😊

↶

⋮

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

Instances (2) Info

Last updated less than a minute ago

Connect

Instance state

Actions

Launch instances

Find Instance by attribute or tag (case-sensitive)

All states

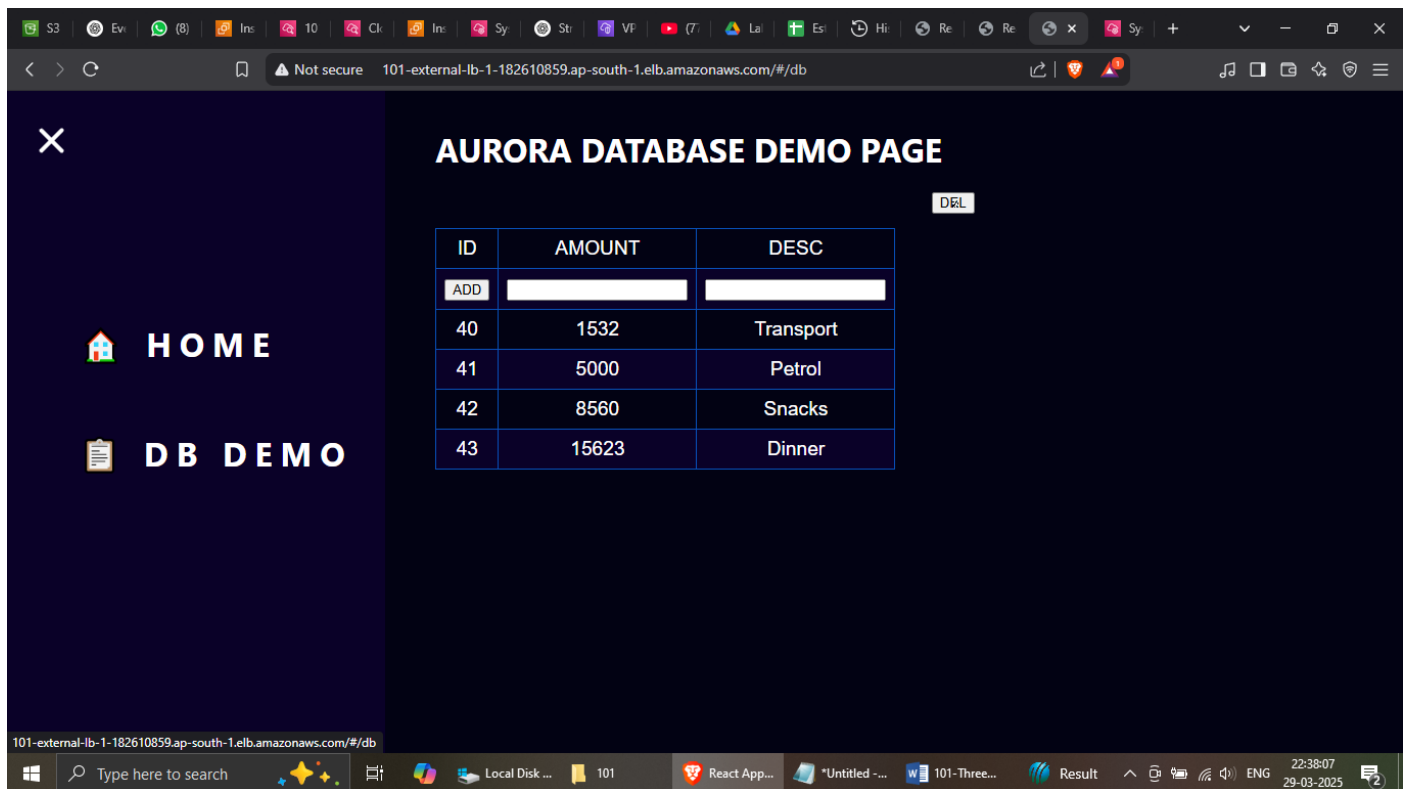
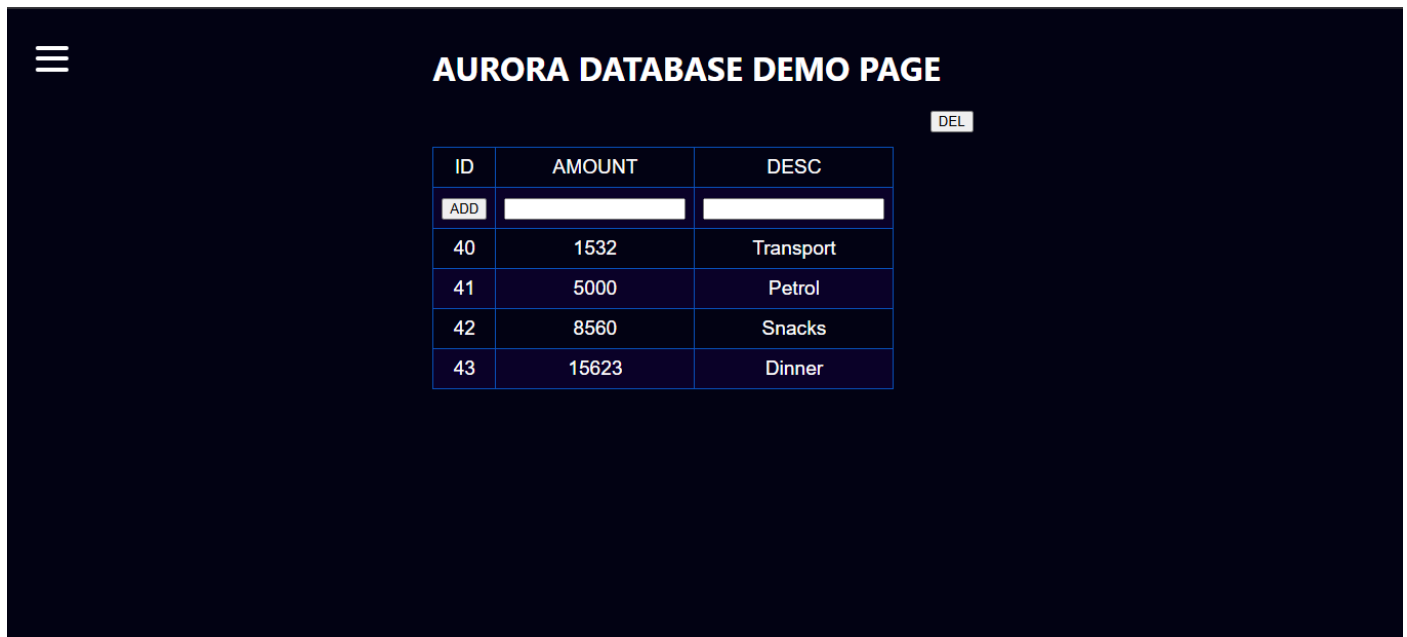
Instance state = running

Clear filters

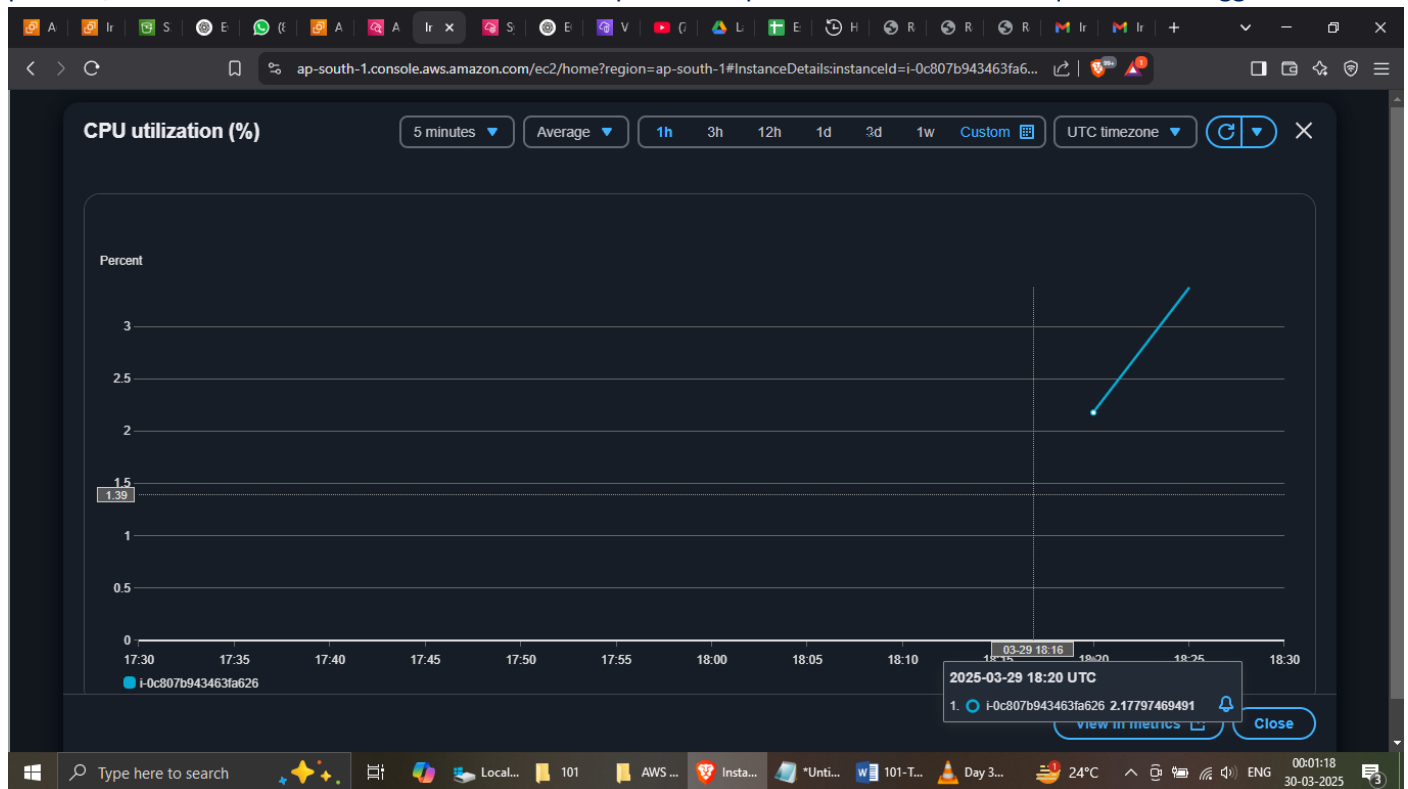
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>		i-0506ca08595516ce6	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a
<input type="checkbox"/>		i-0048b0f7178eedc49	Running	t2.micro	2/2 checks passed	View alarms +	ap-south-1a

'101 - AWS 3 TIER ARCHITECH - BKBALA3710'

© 2011 Pearson Education, Inc. or its affiliate(s). All rights reserved. Printed in the United States of America. This publication is protected by copyright. Any unauthorized distribution, reproduction, or use of this work is illegal. All other rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage or retrieval system, without prior written permission from the copyright owner. Printed on acid-free paper.



21. Initially – CPU utilization 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...



The screenshot shows the AWS CloudWatch 'Alarms' page. The left sidebar contains navigation links for 'Dashboards', 'Alarms', 'Logs', and 'Metrics'. The main content area displays a table of alarms. One alarm is listed: '101-public-app-tier-alarm' with a state of 'OK'. The conditions for this alarm are 'CPUUtilization >= 50 for 1 datapoints within 1 minute'. The page includes filters for 'Alarm state: Any', 'Alarm type: Any', and 'Actions status: Any'. The bottom of the page shows the AWS footer with copyright information and links for 'Privacy', 'Terms', and 'Cookie preferences'.

Name	State	Last state update (UTC)	Conditions
101-public-app-tier-alarm	OK	2025-03-29 18:27:56	CPUUtilization >= 50 for 1 datapoints within 1 minute

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

The screenshot displays the AWS CloudWatch Alarms console. The left sidebar shows navigation options: CloudWatch, Alarms, Favorites and recents, Dashboards, Alarms (0 in alarm, 0 All alarms), Logs (Log groups, Log Anomalies, Live Tail, Logs Insights, Contributor Insights), and Metrics (All metrics). The main panel shows 'Alarms (1)' with a search bar containing '101-public-app-tier-alarm'. The alarm is listed in a table with columns: Name, State, Last state update (UTC), Conditions, and Actions. The alarm '101-public-app-tier-alarm' is in the 'In alarm' state, with a last state update of '2025-03-29 18:33:56'. The condition is 'CPUUtilization >= 50 for 1 datapoints within 1 minute'. The bottom of the screen shows the Windows taskbar with various application icons and the system clock indicating 00:04:02 on 30-03-2025.

Name	State	Last state update (UTC)	Conditions	Actions
101-public-app-tier-alarm	In alarm	2025-03-29 18:33:56	CPUUtilization >= 50 for 1 datapoints within 1 minute	

*Auto scaling performed as a result of alarm

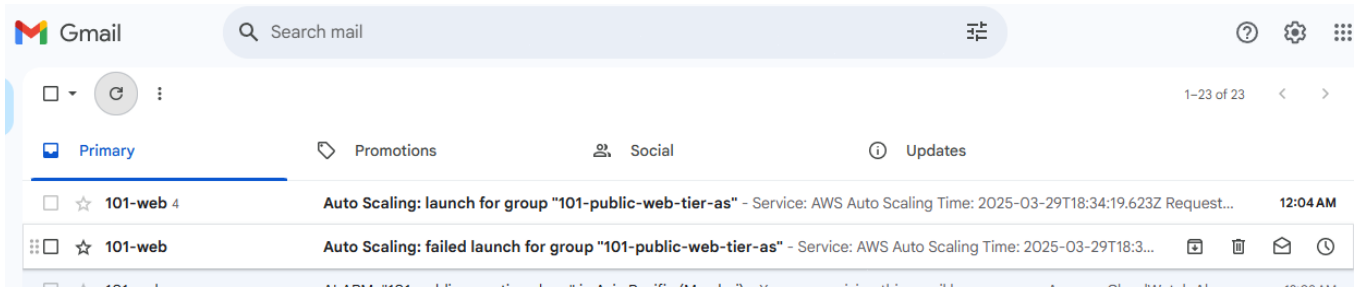
The screenshot shows the AWS Management Console for the 'ap-south-1' region. The 'Instances' page displays 3 EC2 instances in a 'running' state. The instances are t2.micro type, located in the 'ap-south-1a' and 'ap-south-1b' availability zones. The first two instances are in 'ap-south-1a' and the third is in 'ap-south-1b'. The first two instances have '2/2 checks passed' and the third is 'Initializing'. The 'Alarm status' for the first two is 'View alarms' and for the third is '1 in alarm'.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
	i-0048b0f7178eedc49	Running	t2.micro	2/2 checks passed	View alarms	ap-south-1a
	i-0c807b943463fa626	Running	t2.micro	2/2 checks passed	1 in alarm	ap-south-1a
	i-03f66c9f0def5f746	Running	t2.micro	Initializing	View alarms	ap-south-1b

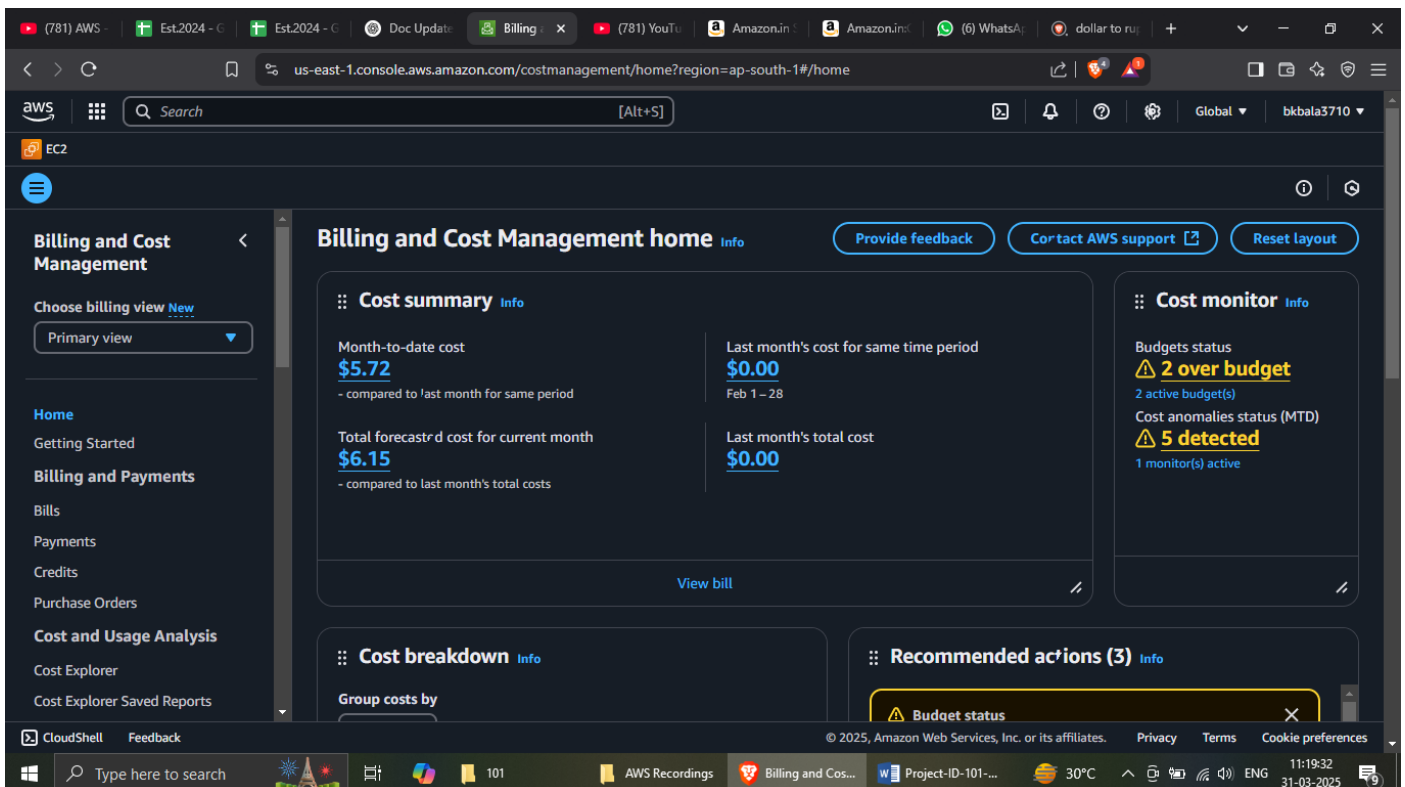
The screenshot shows the AWS Management Console for the 'ap-south-1' region. The 'Instances' page displays 5 EC2 instances in a 'running' state. The instances are t2.micro type, located in the 'ap-south-1a' and 'ap-south-1b' availability zones. The first two instances are in 'ap-south-1a' and the third is in 'ap-south-1b'. The first two instances have '2/2 checks passed' and the third is 'Initializing'. The 'Alarm status' for the first two is 'View alarms' and for the third is '1 in alarm'.

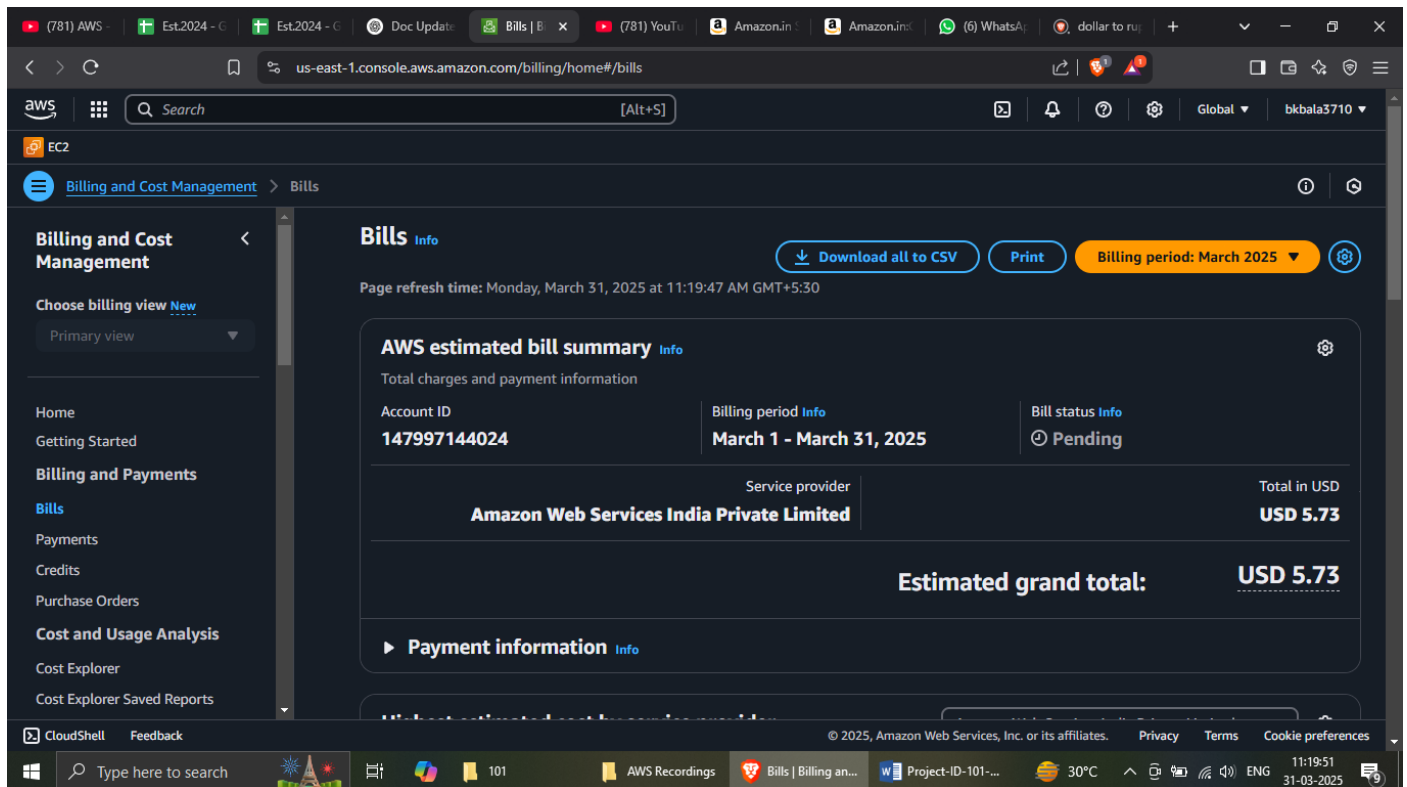
Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Terminated	t2.micro	-	View alarms	ap-south-1a	-
Running	t2.micro	2/2 checks passed	View alarms	ap-south-1a	-
Terminated	t2.micro	-	View alarms	ap-south-1a	-
Running	t2.micro	2/2 checks passed	View alarms	ap-south-1a	-
Running	t2.micro	2/2 checks passed	View alarms	ap-south-1b	-

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 become 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 become 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

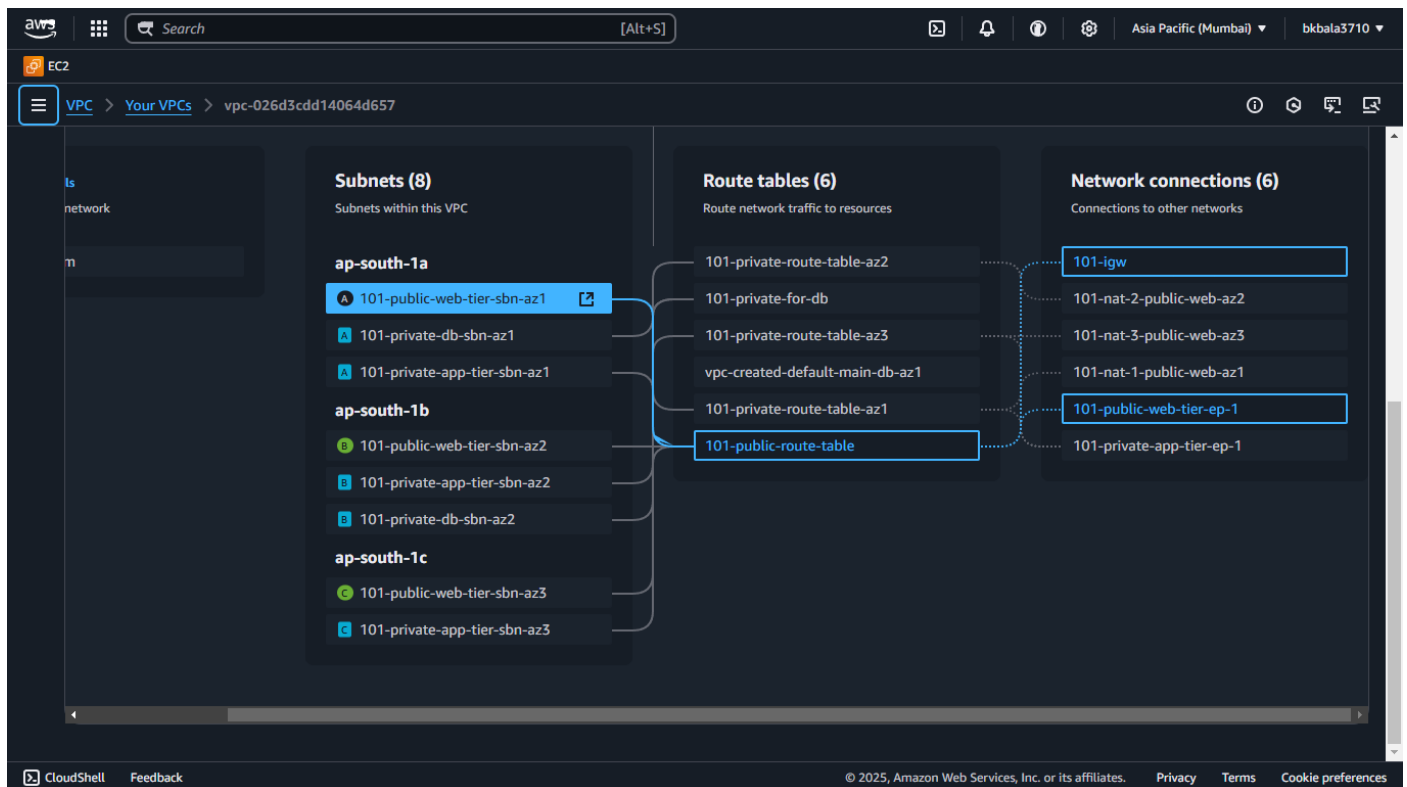
    ctrl + c – come out

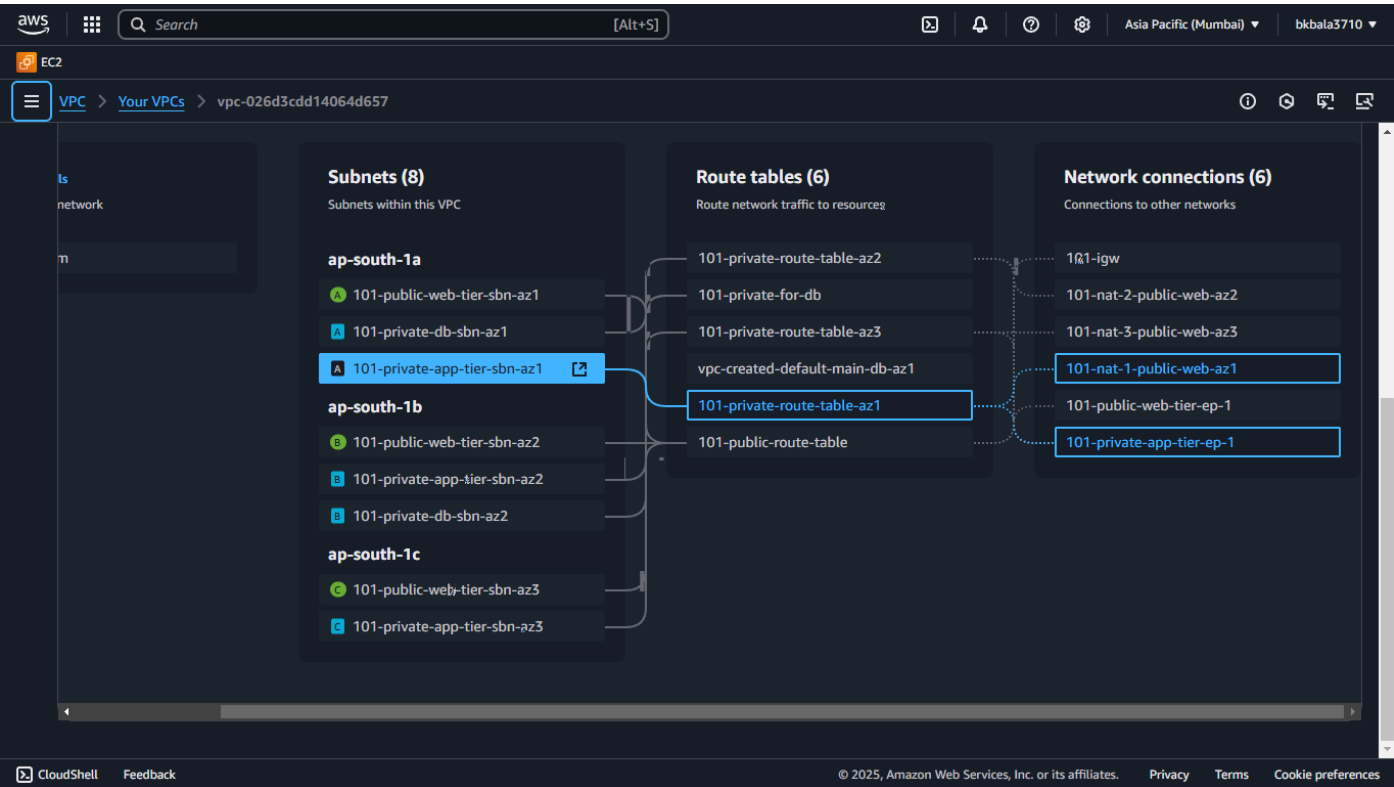
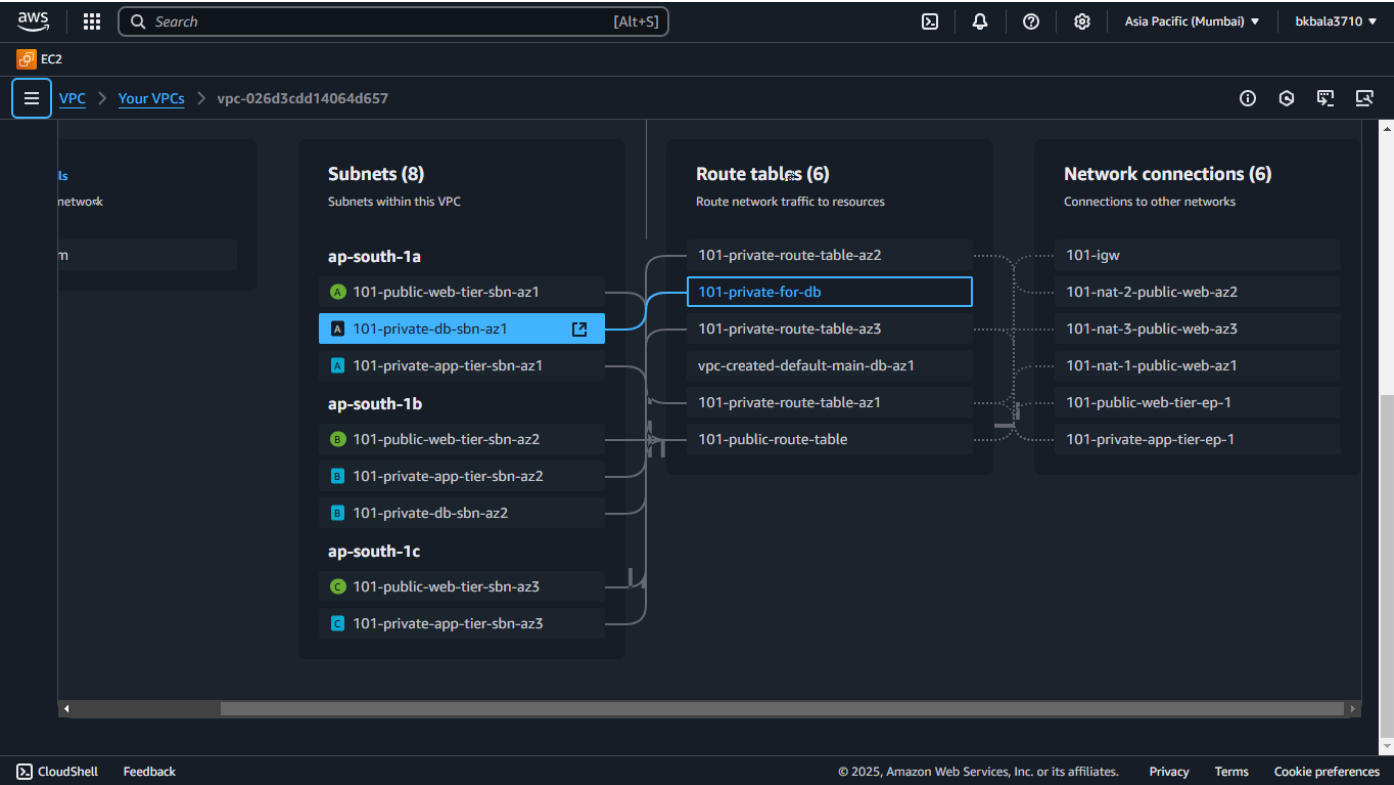
34. pm2 startup
35. pm2 save
36. curl http://localhost:4000/health

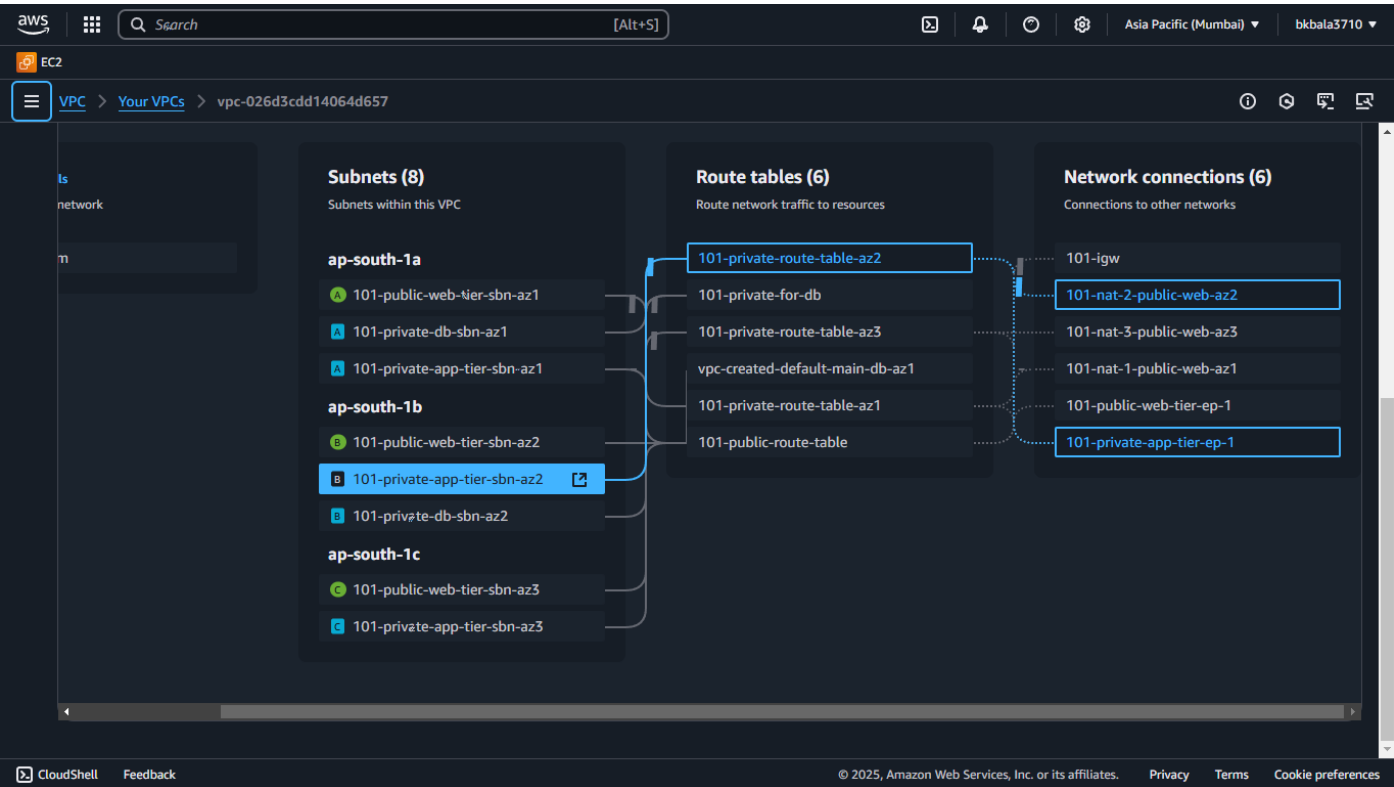
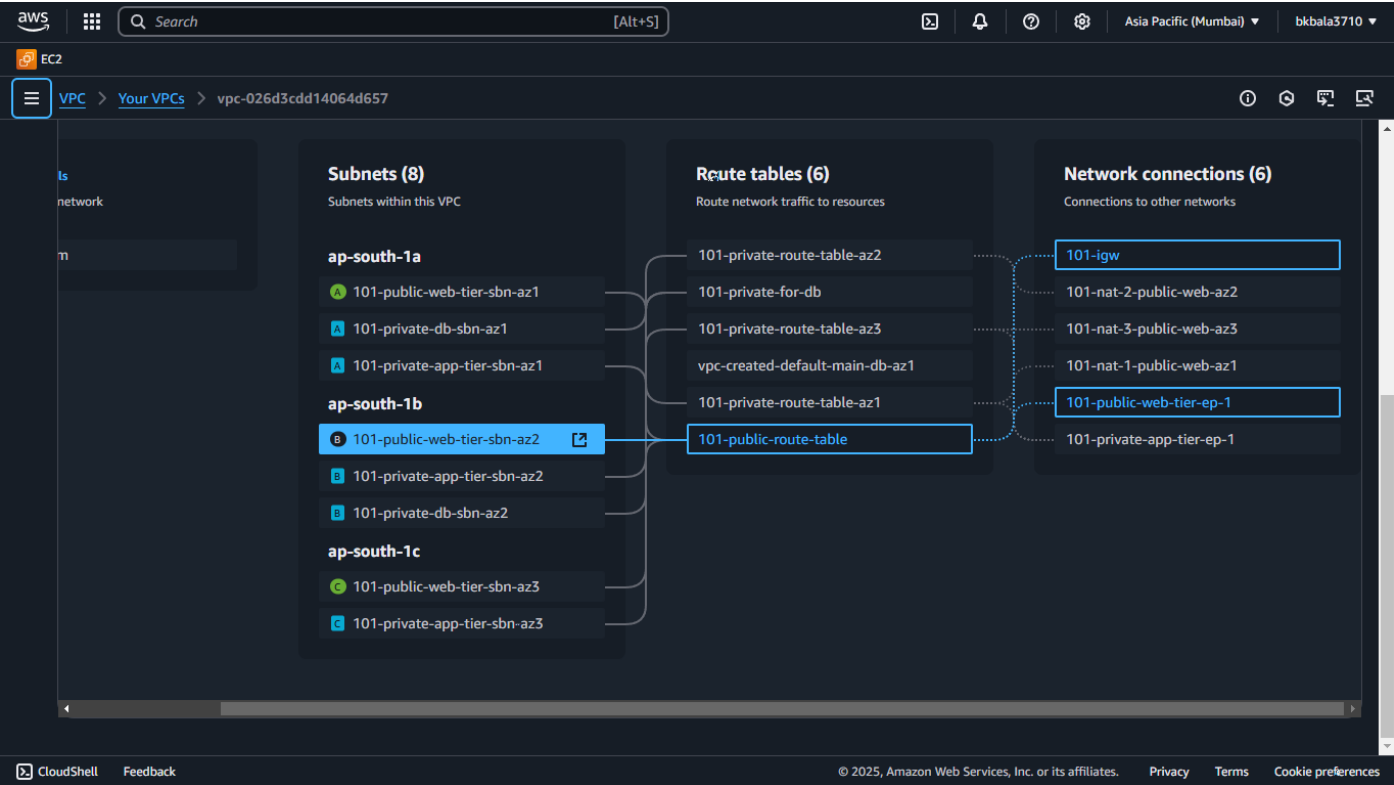
    It should return: This is the health check.

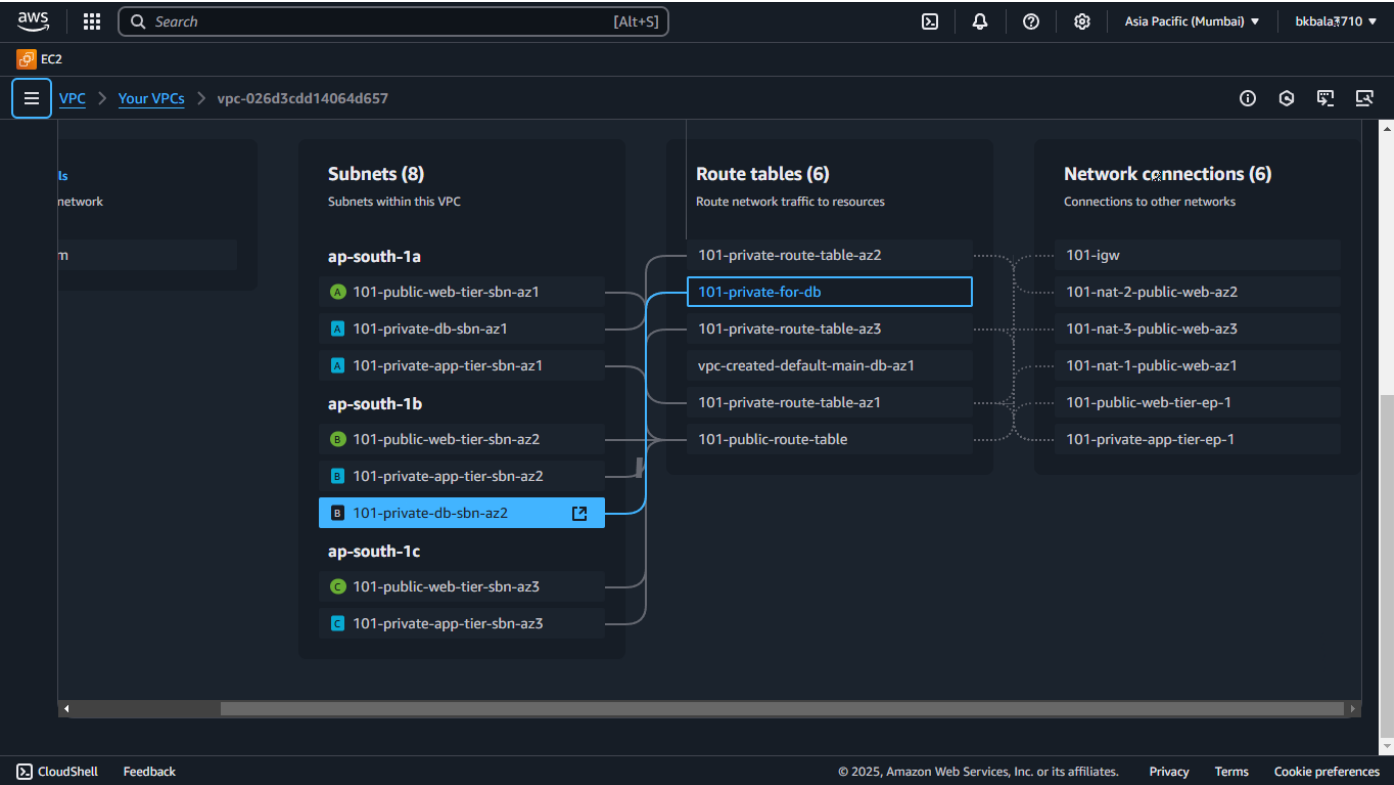
37. Creation of Internal Load Balancer for App Tier ec2 instance
38. Update the nginx.conf file in S3 with internal load balancer DNS.
39. Login to web tier ec2 via SSM system manager – connect (key not required – IAM)
40. sudo -su ec2-user
41. cd /home/ec2-user
42. curl -o- https://raw.githubusercontent.com/avizway1/aws_3tier_architecture/main/install.sh | 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'
```

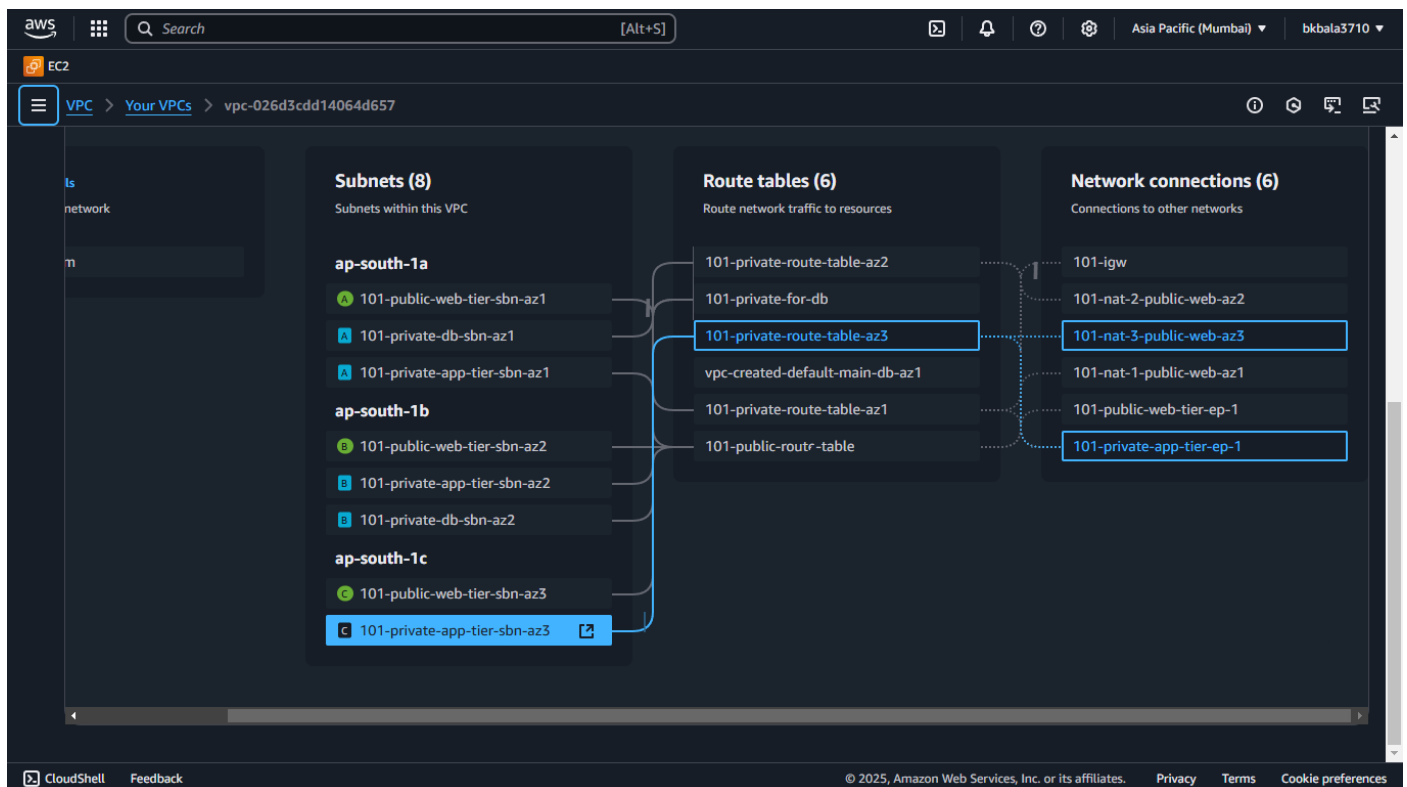
48. cd web-tier
49. npm install
50. npm run build
51. sudo amazon-linux-extras install nginx1 -y
52. cd /etc/nginx (You are in nginx path)
53. ls ----> You will see 'nginx.conf' file
54. sudo rm nginx.conf
55. sudo aws s3 cp s3://<S3 Bucker Name>/application-code/nginx.conf .
Ex: sudo aws s3 cp s3://demo-3tier-project/application-code/nginx.conf .
(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.











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