

## 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.

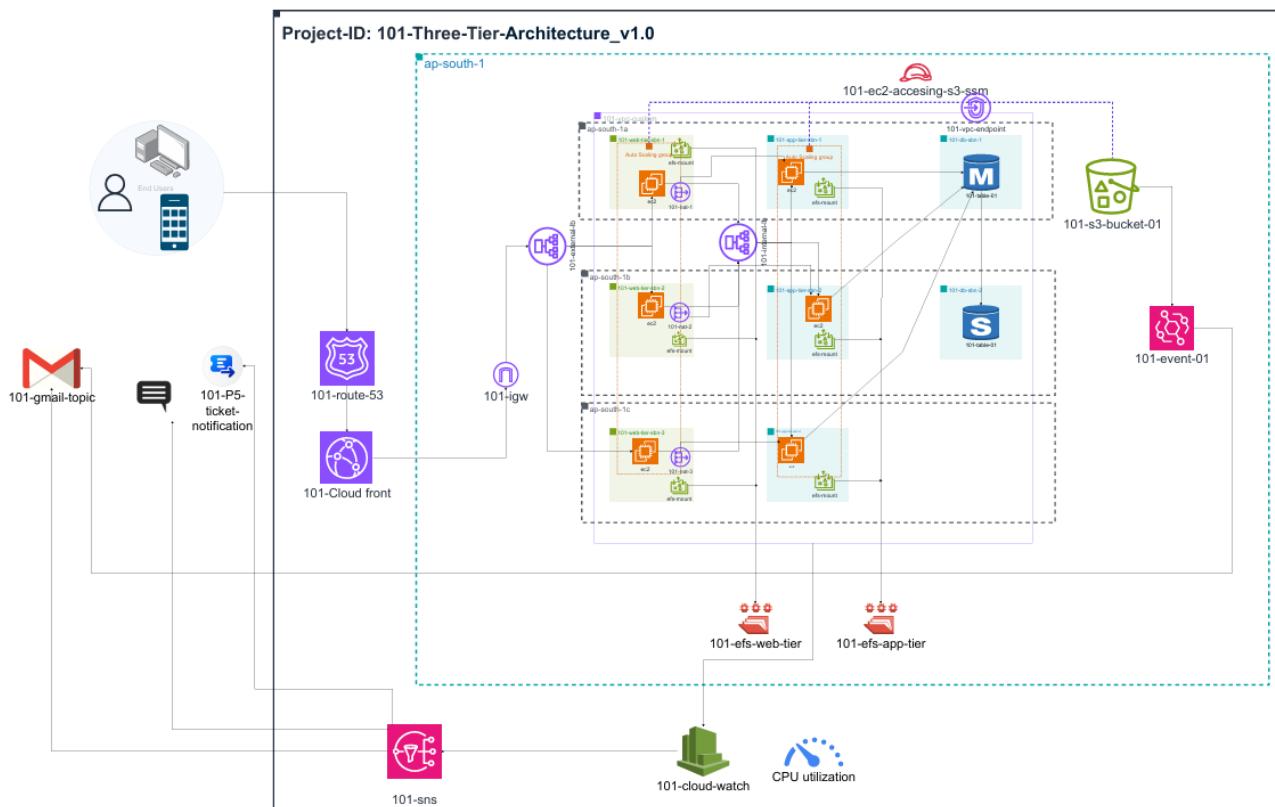
### Architecture flow:

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

**Amazon S3**

**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
- Storage Lens groups

**General purpose buckets (4)**

Buckets are containers for data stored in S3.

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

## 2. VPC – 101-vpc-custom

**Your VPCs (2)**

Last updated less than a minute ago

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

**VPC dashboard**

**Subnets (8)**

Last updated 1 minute ago

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-031bfff9a851e7030	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-089f280234f36aed2	subnet-072e850afc37bc6f7 / 101-private-app-tier-sbn-az3
-	rtb-051a7296504684271	-
vpn-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-026d3cd14064d657   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-0eaee6c3c47f3f2af	3 Subnets	Yes	vpc-05225a81fd9b81e54
-	acl-0800dbde68a4661e5	8 Subnets	Yes	vpc-026d3cd14064d657 /

## 8.1. NACLs - inbound

The screenshot shows the AWS VPC Network ACL inbound rules configuration for a specific Network ACL named 'acl-0800dbde68a4661e5'. The interface includes a sidebar with navigation links for Virtual private cloud, Security (Network ACLs selected), and PrivateLink and. The main panel displays the 'Details' tab with information like Network ACL ID, Associated with 8 Subnets, Default Yes, and VPC ID. Below this, the 'Inbound rules' tab is selected, showing two rules: Rule number 100 (All traffic, All, All, 0.0.0.0/0, Allow) and a wildcard rule (\*) (All traffic, All, All, 0.0.0.0/0, Deny). There are tabs for Outbound rules, Subnet associations, and Tags.

## 8.2. NACLs - Outbound

The screenshot shows the AWS VPC Network ACL outbound rules configuration for the same Network ACL 'acl-0800dbde68a4661e5'. The interface is similar to the inbound rules view, with the 'Outbound rules' tab selected. It lists two rules: Rule number 100 (All traffic, All, All, 0.0.0.0/0, Allow) and a wildcard rule (\*) (All traffic, All, All, 0.0.0.0/0, Deny). The other tabs (Details, Subnet associations, Tags) are also visible.

## 9. Security groups - 5

The screenshot shows the AWS Security Groups list with 7 items. The columns include Name, Security group ID, Security group name, and VPC ID. The security groups listed are:

Name	Security group ID	Security group name	VPC ID
-	<a href="#">sg-0792bff3d1e7df965</a>	default	<a href="#">vpc-05225a81fd9b81e54</a>
101-private-app-sg	<a href="#">sg-0e839d795c1cfecab</a>	101-private-app-sg	<a href="#">vpc-026d3cdd14064d657</a>
-	<a href="#">sg-07942972c8cb62d5c</a>	default	<a href="#">vpc-026d3cdd14064d657</a>
101-private-db-sg	<a href="#">sg-0ba43aea5d1eef9b0</a>	101-private-db-sg	<a href="#">vpc-026d3cdd14064d657</a>
101-external-lb-sg	<a href="#">sg-0c2afcacc5639d415</a>	101-external-lb-sg	<a href="#">vpc-026d3cdd14064d657</a>
101-public-web-sg	<a href="#">sg-052bfaf44e66e7520</a>	101-public-web-sg	<a href="#">vpc-026d3cdd14064d657</a>
101-internal-lb-sg	<a href="#">sg-08b9c9fcfd9bb43933</a>	101-internal-lb-sg	<a href="#">vpc-026d3cdd14064d657</a>

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

**sg-0c2afcacc5639d415 - 101-external-lb-sg**

**Actions ▾**

<b>Details</b>		<b>Security group ID</b>	<b>Description</b>	<b>VPC ID</b>
<b>Security group name</b>	<a href="#">sg-0c2afcacc5639d415</a>	<a href="#">sg-0c2afcacc5639d415</a>	<a href="#">http-access</a>	<a href="#">vpc-026d3cdd14064d657</a>
<b>Owner</b>	<a href="#">147997144024</a>	<b>Inbound rules count</b>	<b>Outbound rules count</b>	
		1 Permission entry	2 Permission entries	

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

**Inbound rules (1)**

[Edit inbound rules](#)

<a href="#">Search</a>	<a href="#">Manage tags</a>	<a href="#">Edit inbound rules</a>				
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 ▾**

<b>Details</b>		<b>Security group ID</b>	<b>Description</b>	<b>VPC ID</b>
<b>Security group name</b>	<a href="#">sg-052bfaf44e66e7520</a>	<a href="#">sg-052bfaf44e66e7520</a>	<a href="#">http only from external lb</a>	<a href="#">vpc-026d3cdd14064d657</a>
<b>Owner</b>	<a href="#">147997144024</a>	<b>Inbound rules count</b>	<b>Outbound rules count</b>	
		2 Permission entries	1 Permission entry	

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

**Inbound rules (2)**

[Edit inbound rules](#)

<a href="#">Search</a>	<a href="#">Manage tags</a>	<a href="#">Edit inbound rules</a>				
Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
sgr-0531e494d9f794f8c	-	HTTP	TCP	80	<a href="#">sg-0c2afcacc5639d415</a> ...	-

### 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 sg-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**

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 sg-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**

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)**

Security group rule ID	IP version	Type	Protocol	Port range	Source	Description
sgr-02cdebc0cd21cc449	-	MySQL/Aurora	TCP	3306	sg-0e839d795c1cf0eab...	-

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

**Endpoints (2) Info**

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

**Actions**    Create endpoint

**Endpoints (2)**

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**

**Actions**

**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)**

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

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

## Policy

VPC endpoint policy controls access to the service

```

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

General purpose buckets (4) [Info](#) [All AWS Regions](#)

Buckets are containers for data stored in S3.

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

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

Session ID: root-kgzpejn9b4pxpq3ybhv2sapzzu Instance ID: i-0506ca08595516ce6

[Terminate](#)

```
[root@ip-10-0-0-193 ec2-user]# aws s3 ls s3://101-app-tier-bucket
An error occurred (AccessDenied) when calling the ListObjectsV2 operation: User: arn:aws:sts::147997144024:assumed-role/101-ec2-accessing-s3-ssm/i-0506ca08595516ce6 is not authorized to perform: s3>ListBucket on resource: "arn:aws:s3:::101-app-tier-bucket" because no VPC endpoint policy allows the s3>ListBucket action
[root@ip-10-0-0-193 ec2-user]#
```

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

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

**Details**

Endpoint ID vpce-00e3d8fb86430d134	Status Available	Creation time Saturday, March 29, 2025 at 19:18:46 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 (3)**

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

**Manage route tables**

\*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 (4)** Info All AWS Regions

Buckets are containers for data stored in S3.

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

only can view app tier bucket as mentioned in policy

```

Session ID: root-
Instance ID: i-0048b0f7178eedc49
Terminate
X

[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

Name	Launch template/configuration	Instances	Status	Desired capacity
<a href="#">101-private-web-tier-as</a>	<a href="#">101-private-app-tier-template</a>   Version D	1	-	1
<a href="#">101-public-web-tier-as</a>	<a href="#">101-public-web-tier-template</a>   Version D	1	-	1

## 11.1 Public-web-tier

**101-public-web-tier-as**

**101-public-web-tier-as Capacity overview**

[Edit](#)

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

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

Details Integrations - new Automatic scaling Instance management Instance refresh Activity

**Launch template**

[Edit](#)

Launch template <a href="#">lt-0a3e36a68d23cae76</a> 101-public-web-tier-template	AMI ID <a href="#">ami-04eed0e618979ba41</a>	Instance type t2.micro	Owner arn:aws:iam::147997144024:root
Version Default	Security groups -	Security group IDs <a href="#">sg-052bfaf44e66e7520</a>	Create time Sat Mar 29 2025 19:05:05 GMT+0530 (India Standard Time)

\*Launch template

**Launch Templates (2) [Info](#)**

[C](#) Actions ▾ [Create launch template](#)

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

### 101-public-web-tier-template (lt-0a3e36a68d23cae76)

[Actions ▾](#) [Delete template](#)

#### Launch template details

Launch template ID <input type="checkbox"/> lt-0a3e36a68d23cae76	Launch template name <input type="checkbox"/> 101-public-web-tier-template	Default version <input type="checkbox"/> 1	Owner <input type="checkbox"/> arn:aws:iam::147997144024:root
---	---	---	--

[Details](#) [Versions](#) [Template tags](#)

#### Launch template version details

[Actions ▾](#) [Delete template version](#)

Version 1 (Default) ▾	Description <input type="checkbox"/> 101-public-web-tier-template-desc	Date created <input type="checkbox"/> 2025-03-29T13:35:05.000Z	Created by <input type="checkbox"/> arn:aws:iam::147997144024:root
<a href="#">Instance details</a> <a href="#">Storage</a> <a href="#">Resource tags</a> <a href="#">Network interfaces</a> <a href="#">Advanced details</a>			
AMI ID <input type="checkbox"/> ami-04eed0e618979ba41	Instance type <input type="checkbox"/> t2.micro	Availability Zone -	Key pair name -
Security groups -	Security group IDs <input type="checkbox"/> sg-052bfaf44e66e7520		

### 101-Simple-Scaling-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

[Edit](#)

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

[Edit](#)

Launch template	AMI ID	Instance type	Owner
<a href="#">lt-045ddec48d7896ee5</a> 101-private-app-tier-template	<a href="#">ami-0c373e3995666b7bb</a>	t2.micro	arn:aws:iam::147997144024:root
Version	Security groups	Security group IDs	Create time
Default	-	<a href="#">sg-0e839d795c1cf0eab</a>	Sat Mar 29 2025 19:06:55 GMT+0530 (India Standard Time)

\*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"/>	<a href="#">lt-045ddec48d7896ee5</a>	101-private-app-tier-template	1	1	2025-03-29T13:36:55.000Z
<input type="checkbox"/>	<a href="#">lt-0a3e36a68d23cae76</a>	101-public-web-tier-template	1	1	2025-03-29T13:35:05.000Z

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

[Actions ▾](#) [Delete template](#)

**Launch template details**

Launch template ID <input type="checkbox"/> lt-045ddec48d7896ee5	Launch template name <input type="checkbox"/> 101-private-app-tier-template	Default version <input type="checkbox"/> 1	Owner <input type="checkbox"/> arn:aws:iam::147997144024:root
---	--	---	--

[Details](#) [Versions](#) [Template tags](#)

**Launch template version details**

Version 1 (Default) ▾	Description <input type="checkbox"/> 101-private-app-tier-template-desc	Date created <input type="checkbox"/> 2025-03-29T13:36:55.000Z	Created by <input type="checkbox"/> arn:aws:iam::147997144024:root	
Instance details	Storage	Resource tags	Network interfaces	Advanced details
AMI ID <input type="checkbox"/> ami-0c373e3995666b7bb	Instance type <input type="checkbox"/> t2.micro	-	Availability Zone -	Key pair name -
Security groups -	Security group IDs <input type="checkbox"/> sg-0e839d795c1cf0eab	-	-	-

**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.

The screenshot shows the Gmail inbox with the 'Primary' tab selected. There are 10 new messages in the 'Promotions' folder. The messages are all from 'Autodesk' and relate to AWS Auto Scaling events for groups like '101-private-web-tier-as' and '101-public-web-tier-as'. The messages include details such as launch, failed launch, test notification, and termination events, along with their respective times and request IDs.

			1-20 of 20
			< >
<input checked="" type="checkbox"/>	Primary	Promotions 10 new Autodesk — Get and keep client...	
<input type="checkbox"/>	101-app	Auto Scaling: launch for group "101-private-web-tier-as" - Service: AWS Auto Scaling Time: 2025-03-29T13:40:38.486Z RequestId:...	7:10 PM
<input type="checkbox"/>	101-app	Auto Scaling: failed launch for group "101-private-web-tier-as" - Service: AWS Auto Scaling Time: 2025-03-29T13:40:20.959Z Req...	7:10 PM
<input type="checkbox"/>	101-app	Auto Scaling: test notification for group "101-private-web-tier-as" - Service: AWS Auto Scaling Time: 2025-03-29T13:40:16.458Z R...	7:10 PM
<input type="checkbox"/>	101-web	Auto Scaling: launch for group "101-public-web-tier-as" - Service: AWS Auto Scaling Time: 2025-03-29T13:39:18.440Z RequestId: ...	7:09 PM
<input type="checkbox"/>	101-web	Auto Scaling: test notification for group "101-public-web-tier-as" - Service: AWS Auto Scaling Time: 2025-03-29T13:38:44.742Z Re...	7:08 PM
<input type="checkbox"/>	101-web	Auto Scaling: termination for group "101-public-web-tier-as" - Service: AWS Auto Scaling Time: 2025-03-29T13:27:42.723Z Reques...	6:57 PM
<input type="checkbox"/>	101-app	Auto Scaling: termination for group "101-private-app-tier-as" - Service: AWS Auto Scaling Time: 2025-03-29T13:27:04.026Z Reque...	6:57 PM

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

The screenshot shows the AWS Lambda console with the search bar set to 'Owned by me'. It lists two Lambda functions: 'public image' and 'private-image'. Each function has its ARN, last updated time ('less than a minute ago'), and owner ('147997144024') displayed.

Amazon Machine Images (AMIs) (2) <a href="#">Info</a>				
<a href="#">Owned by me</a>		<a href="#">Find AMI by attribute or tag</a>		
<input type="checkbox"/>	Name	AMI name	AMI ID	Source
<input type="checkbox"/>	public image	ami-04eed0e618979ba41	147997144024/public image	147997144024
<input type="checkbox"/>	private-image	ami-0c373e3995666b7bb	147997144024/private-image	147997144024

## 13 . Snapshot of AMI

The screenshot shows the AWS Lambda console with the search bar set to 'Owned by me'. It lists two Lambda functions: 'public image' and 'private-image'. Each function has its ARN, last updated time ('less than a minute ago'), and owner ('147997144024') displayed.

Snapshots (2) <a href="#">Info</a>				
<a href="#">Owned by me</a>		<a href="#">Search</a>		
<input type="checkbox"/>	Name	Snapshot ID	Full snapshot size	Volume size
<input type="checkbox"/>	-	snap-0f302180b6361fe12	2.91 GiB	8 GiB
<input type="checkbox"/>	-	snap-0bc0182347484b000	2.04 GiB	8 GiB

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

The screenshot shows the AWS Lambda console with the search bar set to 'Owned by me'. It lists two Lambda functions: 'public image' and 'private-image'. Each function has its ARN, last updated time ('less than a minute ago'), and owner ('147997144024') displayed.

Volumes (2) <a href="#">Info</a>							
<a href="#">Saved filter sets</a>		<a href="#">Choose filter set</a>		<a href="#">Search</a>		<a href="#">Actions</a>	
<input type="checkbox"/>	Name	Volume ID	Type	Size	IOPS	Throughput	Snapshot ID
<input type="checkbox"/>	-	vol-04060ad4e6236af43	gp2	8 GiB	100	-	snap-0f30218...
<input type="checkbox"/>	-	vol-016a26f83ae017ee	gp2	8 GiB	100	-	snap-0bc0182...

## 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.								
<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.amazonaws.com	Active	vpc-026d3cdd14064d657	3 Availability zones	100% healthy	100% healthy	
<input type="checkbox"/>	101-external-lb-1	101-external-lb-1-182610859.ap-south-1.elb.amazonaws.com	Active	vpc-026d3cdd14064d657	3 Availability zones	100% healthy	100% healthy	

### 15.1 LB corresponding target groups

Target groups (2) <a href="#">Info</a>						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							
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	<a href="#">vpc-026d3cdd14064d657</a>
IP address type	IPv4	Load balancer	<a href="#">101-external-lb-1</a>				
1 Total targets	1 Healthy	0 Unhealthy	0 Unused	0 Initial	0 Draining		
	0 Anomalous						

101-internal-lb-tg-1							
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	<a href="#">vpc-026d3cdd14064d657</a>
IP address type	IPv4	Load balancer	<a href="#">101-internal-lb-1</a>				
1 Total targets	1 Healthy	0 Unhealthy	0 Unused	0 Initial	0 Draining		
	0 Anomalous						

## 16. RDS database

Databases (1)

Filter by databases

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

Aurora and RDS < sbngrp01-101

**Subnet group details**

- VPC ID: vpc-026d3cd14064d657
- ARN: arn:aws:rds:ap-south-1:147997144024:subgrp:sbngrp01-101
- Supported network types: IPv4
- Description: sbngrp01-101

**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**

**Details** Info

Route table ID: rtb-0c7eb77850db1492a	Main: No	Explicit subnet associations: 3 subnets	Edge associations: -
VPC: vpc-026d3cd14064d657   101-vpc-custom	Owner ID: 147997144024		

**Routes** Subnet associations Edge associations Route propagation Tags

**Routes (3)**

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 ▾**

<b>Details</b> <a href="#">Info</a>		Main <input checked="" type="checkbox"/> Yes	Explicit subnet associations -	Edge associations -
Route table ID <a href="#">rtb-03eb92087bcc9375b</a>	VPC <a href="#">vpc-026d3cdd14064d657   101-vpc-custom</a>	Owner ID <a href="#">147997144024</a>		

**Routes** **Subnet associations** **Edge associations** **Route propagation** **Tags**

**Routes (1)**

**Filter routes** **Both** **Edit routes**

Destination	Target	Status	Propagated
10.0.0.0/16	local	<input checked="" type="checkbox"/> 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 ▾**

<b>Details</b> <a href="#">Info</a>		Main <input type="checkbox"/> No	Explicit subnet associations <a href="#">subnet-04b4a11e675f9a680 / 101-private-app-tier-sbn-az1</a>	Edge associations -
Route table ID <a href="#">rtb-02f196a3f71fdc6b1</a>	VPC <a href="#">vpc-026d3cdd14064d657   101-vpc-custom</a>	Owner ID <a href="#">147997144024</a>		

**Routes** **Subnet associations** **Edge associations** **Route propagation** **Tags**

**Routes (3)**

**Filter routes** **Both** **Edit routes**

Destination	Target	Status	Propagated
<a href="#">pl-78a54011</a>	<a href="#">vpce-00e3d8fb86430d134</a>	<input checked="" type="checkbox"/> Active	No
0.0.0.0/0	<a href="#">nat-08d74c56eaeb3318</a>	<input checked="" type="checkbox"/> Active	No
10.0.0.0/16	local	<input checked="" type="checkbox"/> 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	Main	Explicit subnet associations	Edge associations
<a href="#">rtb-09273bb3477243a20</a>	<input type="checkbox"/> No	subnet-0ac8791286e5ada0e / 101-private-app-tier-sbn-az2	-
VPC	Owner ID		
vpc-026d3cdd14064d657   101-vpc-custom	<a href="#">147997144024</a>		

[Routes](#)
[Subnet associations](#)
[Edge associations](#)
[Route propagation](#)
[Tags](#)

#### Routes (3)

[Filter routes](#)
[Both ▾](#)
[Edit routes](#)

Destination	Target	Status	Propagated
<a href="#">pl-78a54011</a>	<a href="#">vpce-00e3d8fb86430d134</a>	<span>Active</span>	No
0.0.0.0/0	<a href="#">nat-05a7cce02f722b86a</a>	<span>Active</span>	No
10.0.0.0/16	local	<span>Active</span>	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	Main	Explicit subnet associations	Edge associations
<a href="#">rtb-088f280234f36aed2</a>	<input type="checkbox"/> No	subnet-072e850afc37bc6f7 / 101-private-app-tier-sbn-az3	-
VPC	Owner ID		
vpc-026d3cdd14064d657   101-vpc-custom	<a href="#">147997144024</a>		

[Routes](#)
[Subnet associations](#)
[Edge associations](#)
[Route propagation](#)
[Tags](#)

#### Routes (3)

[Filter routes](#)
[Both ▾](#)
[Edit routes](#)

Destination	Target	Status	Propagated
<a href="#">pl-78a54011</a>	<a href="#">vpce-00e3d8fb86430d134</a>	<span>Active</span>	No
0.0.0.0/0	<a href="#">nat-0813175a15a3c2f69</a>	<span>Active</span>	No
10.0.0.0/16	local	<span>Active</span>	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

<b>Route table ID</b> rtb-06ad185397e934c78	<b>Main</b> No	<b>Explicit subnet associations</b> 2 subnets	<b>Edge associations</b> -
<b>VPC</b> vpc-026d3cdd14064d657   101-vpc-custom	<b>Owner ID</b> 147997144024		

**Routes** **Subnet associations** **Edge associations** **Route propagation** **Tags**

**Routes (1)**

Destination		Target	Status	Propagated
10.0.0.0/16		local	Active	No

## 18. Topic & subscriptions

**Amazon SNS** > **Topics**

**Topics (2)**

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)**

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) [Inbox x](#)

 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:

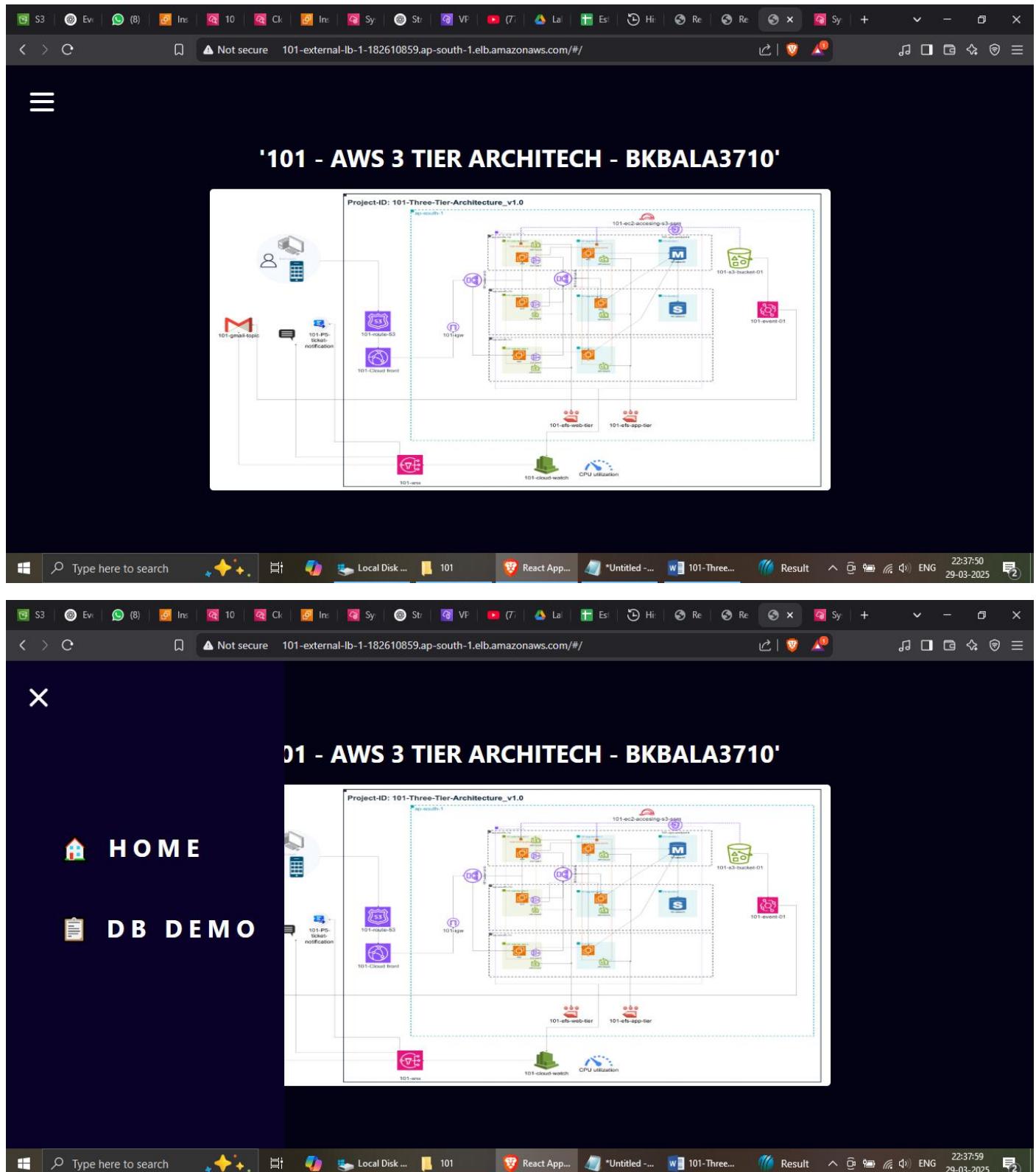
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 50.0 for at least 1 of the last 1 period(s) of 60 seconds.

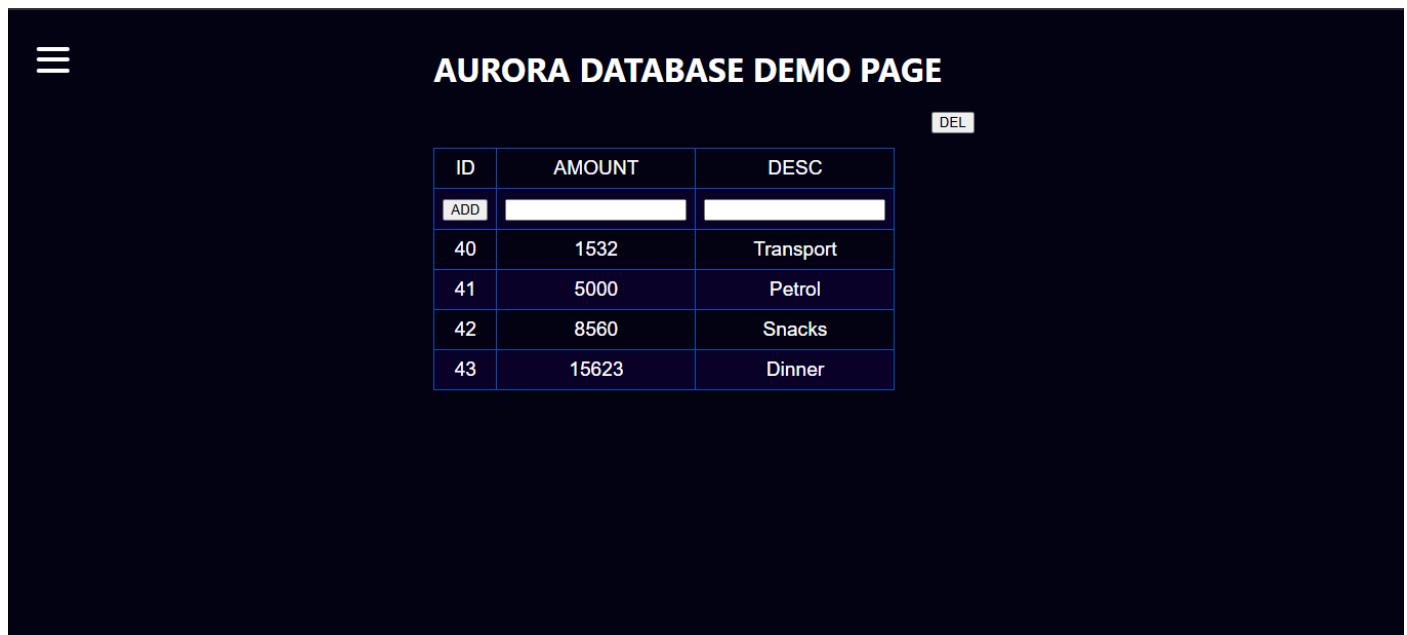
Monitored Metric:

## 19. EC2 right running only 2 instance

Instances (2) <a href="#">Info</a>		Last updated  less than a minute ago		<a href="#">Connect</a>	<a href="#">Instance state ▾</a>	<a href="#">Actions ▾</a>	<a href="#">Launch instances</a>	
		 Find Instance by attribute or tag (case-sensitive)		<a href="#">All states ▾</a>				
<input type="checkbox"/>	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	<a href="#">View alarms +</a>	ap-south-1a	
<input type="checkbox"/>		i-0048b0f7178eedc49	 Running  	t2.micro	 2/2 checks passed	<a href="#">View alarms -</a>	ap-south-1a	

## 20. Demo





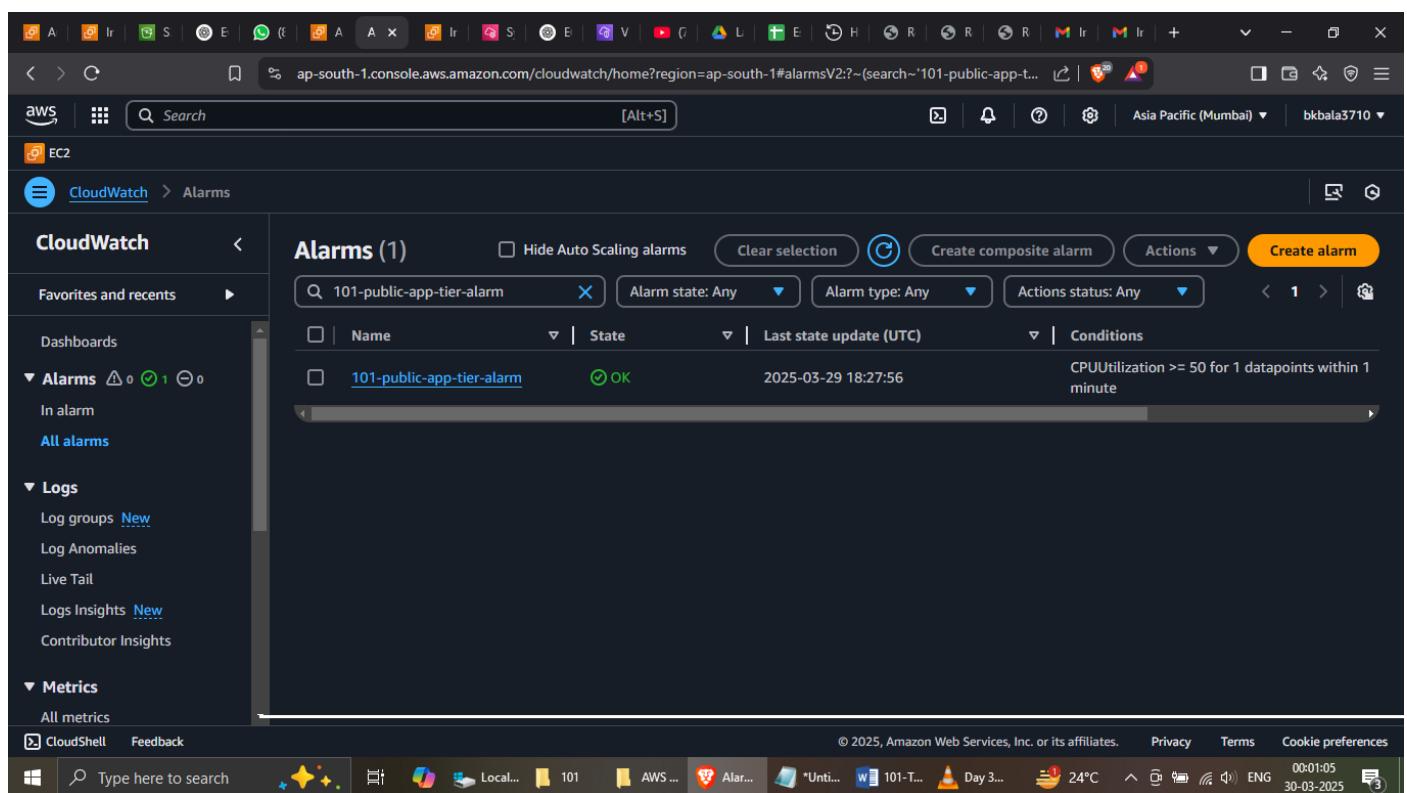
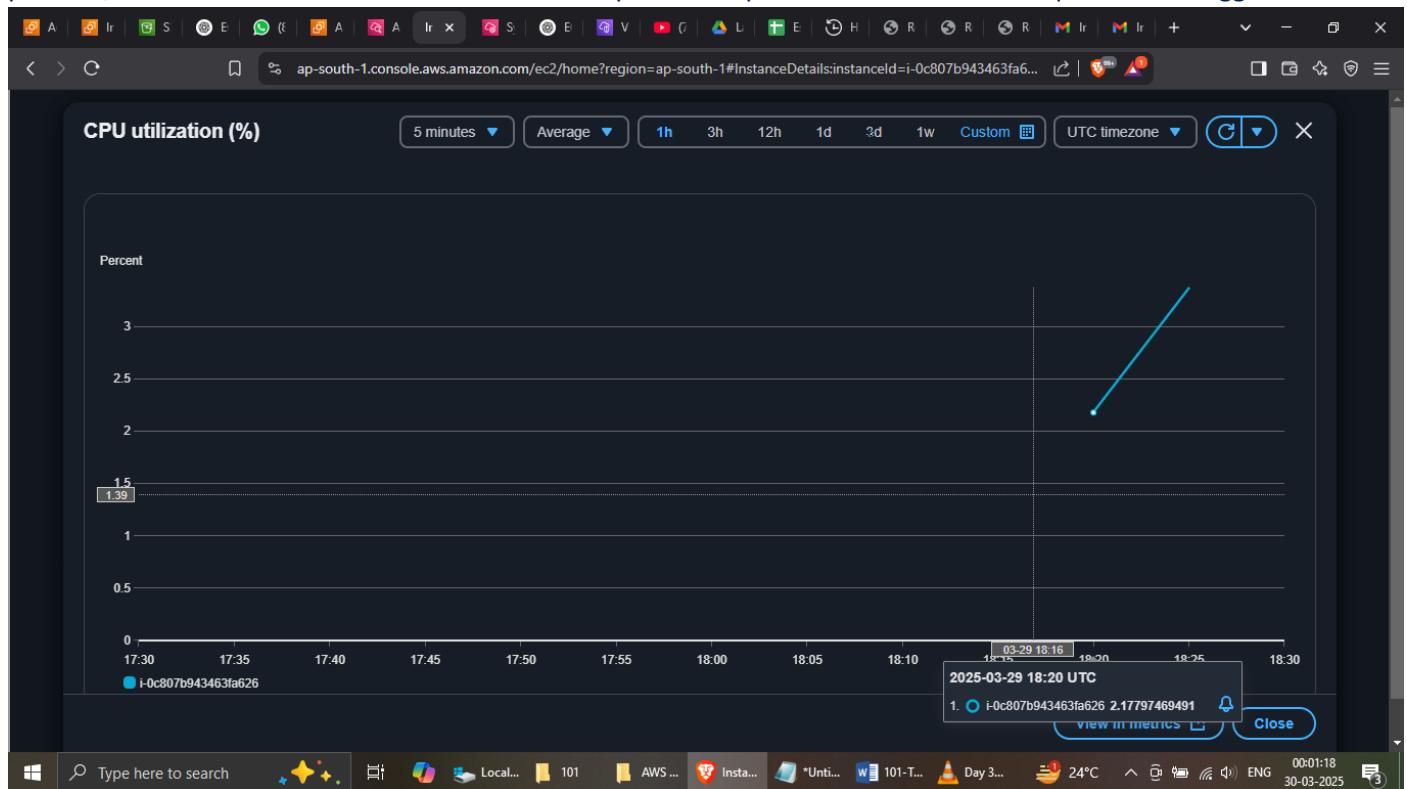
A screenshot of a web browser window showing the "AURORA DATABASE DEMO PAGE". The browser address bar indicates the URL is "101-external-lb-1-182610859.ap-south-1.elb.amazonaws.com/#/db". The page title is "AURORA DATABASE DEMO PAGE".

The browser interface includes a navigation bar with various icons and a toolbar with additional icons. On the left side of the browser window, there is a sidebar with two items: "HOME" and "DB DEMO", each accompanied by a small icon.

The main content area displays the same table as the first screenshot, showing the same five rows of data. A "DEL" button is located at the top right of the table.

The bottom of the screen shows the Windows taskbar with several open application windows and system status indicators.

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...



## 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 shows the AWS CloudWatch Alarms interface. On the left, there's a navigation sidebar with sections for CloudWatch, Favorites and recents, Dashboards, Alarms (selected), Logs, and Metrics. The main area displays a table for alarms:

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

At the top of the main area, there are filters for Hide Auto Scaling alarms, Clear selection, Create composite alarm, Actions, and a Create alarm button. The search bar at the top also contains the alarm name.

\*Auto scaling performed as a result of alarm

The screenshot shows the AWS EC2 Instances page. There are three instances listed:

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

A dropdown menu is open, showing the message "Select an instance".

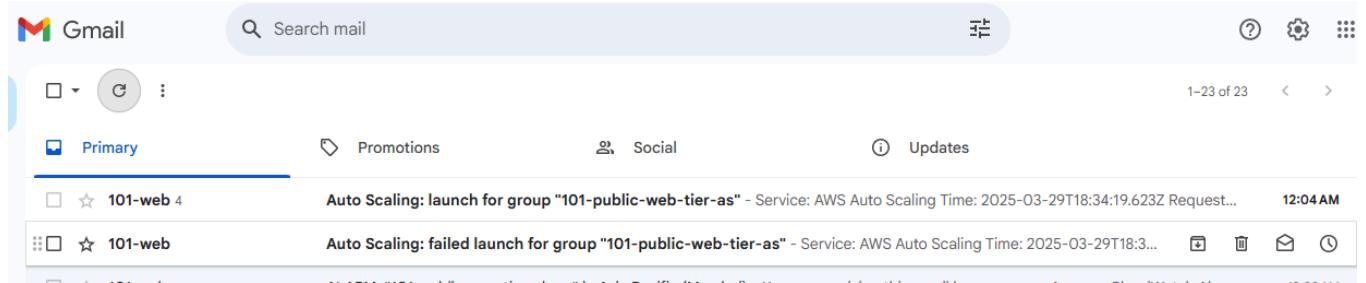
  

The screenshot shows the AWS EC2 Instances page. There are five instances listed:

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

A dropdown menu is open, showing the message "Select an instance".

## 21.2 Auto scaling triggered SNS



## 22. Cost Management

The screenshot shows the AWS Billing and Cost Management home page with the following sections:

- Billing and Cost Management:** Choose billing view New Primary view
- Home:** Getting Started, Billing and Payments, Bills, Payments, Credits, Purchase Orders, Cost and Usage Analysis, Cost Explorer, Cost Explorer Saved Reports
- Billing and Cost Management home:** Info, Provide feedback, Contact AWS support, Reset layout
- Cost summary:** Month-to-date cost \$5.72 (compared to last month for same period), Total forecasted cost for current month \$6.15 (compared to last month's total costs), Last month's cost for same time period \$0.00 (Feb 1 – 28), Last month's total cost \$0.00, View bill
- Cost monitor:** Budgets status, 2 over budget (2 active budget(s)), Cost anomalies status (MTD), 5 detected (1 monitor(s) active)
- Cost breakdown:** Group costs by
- Recommended actions (3):** Budget status (with a warning icon)

At the bottom, there is a navigation bar with CloudShell, Feedback, AWS Recordings, Project-ID-101..., 30°C, ENG, 11:19:32, 31-03-2025, and a notification icon.

The screenshot shows the AWS Billing and Cost Management console. The left sidebar is titled "Billing and Cost Management" and includes links for Home, Getting Started, Billing and Payments, Bills (selected), Payments, Credits, Purchase Orders, Cost and Usage Analysis, Cost Explorer, and Cost Explorer Saved Reports. The main content area is titled "Bills" and displays the "AWS estimated bill summary". The summary table includes the following data:

Account ID	Billing period Info	Bill status Info
147997144024	March 1 - March 31, 2025	Pending
Service provider		Total in USD
Amazon Web Services India Private Limited		USD 5.73
		<b>Estimated grand total:</b>
		<b>USD 5.73</b>

Below the summary, there is a section titled "Payment information". The bottom of the screen shows the Windows taskbar with various icons and the system tray.

## 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>

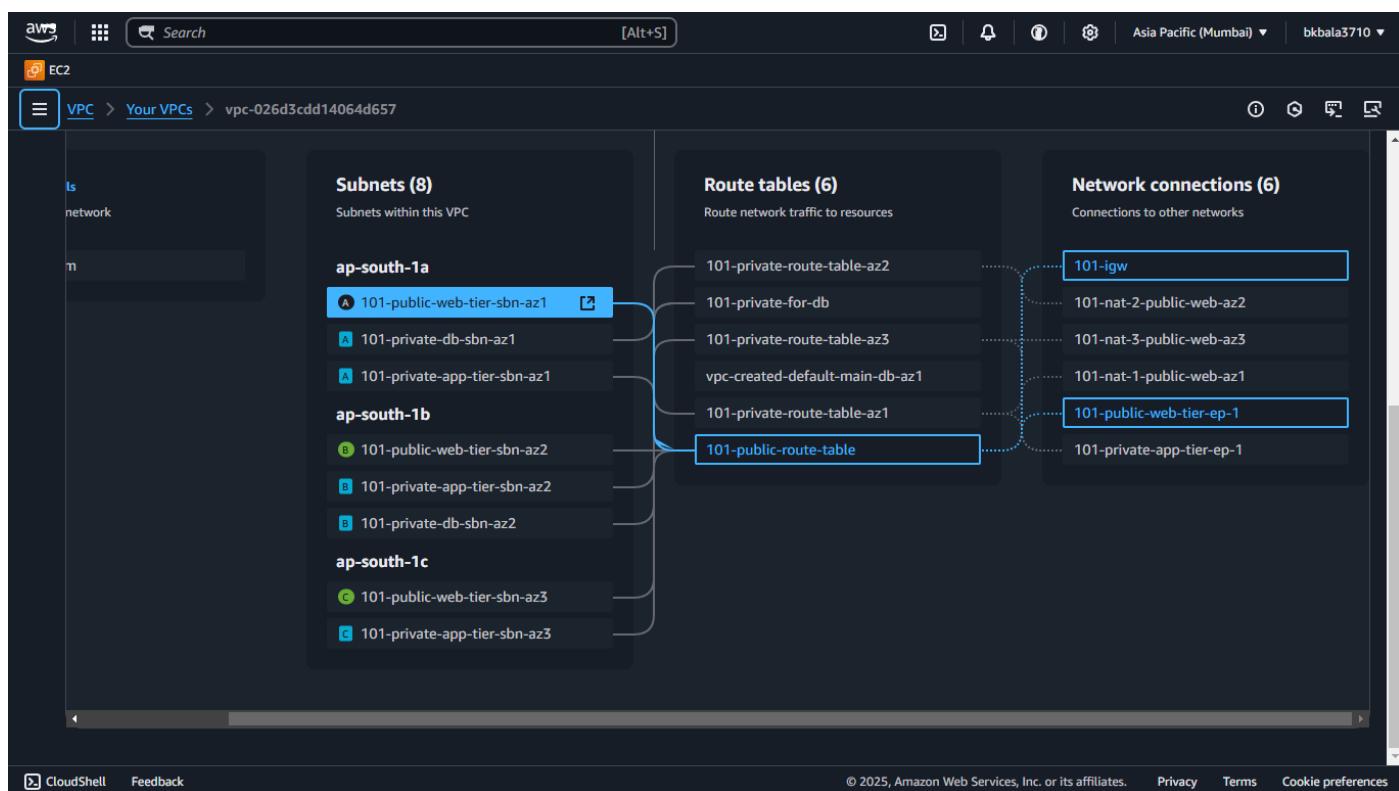
ctrl + c – come out

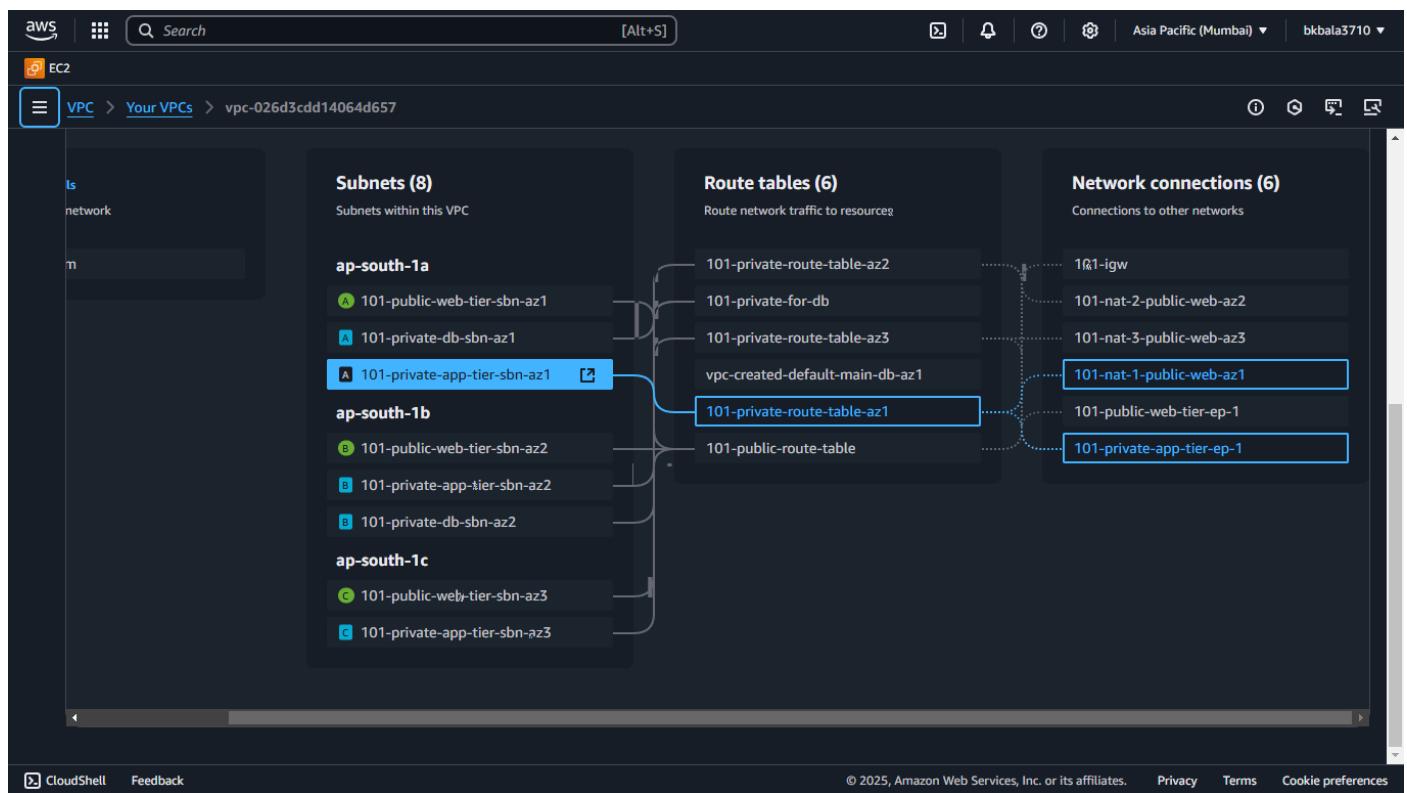
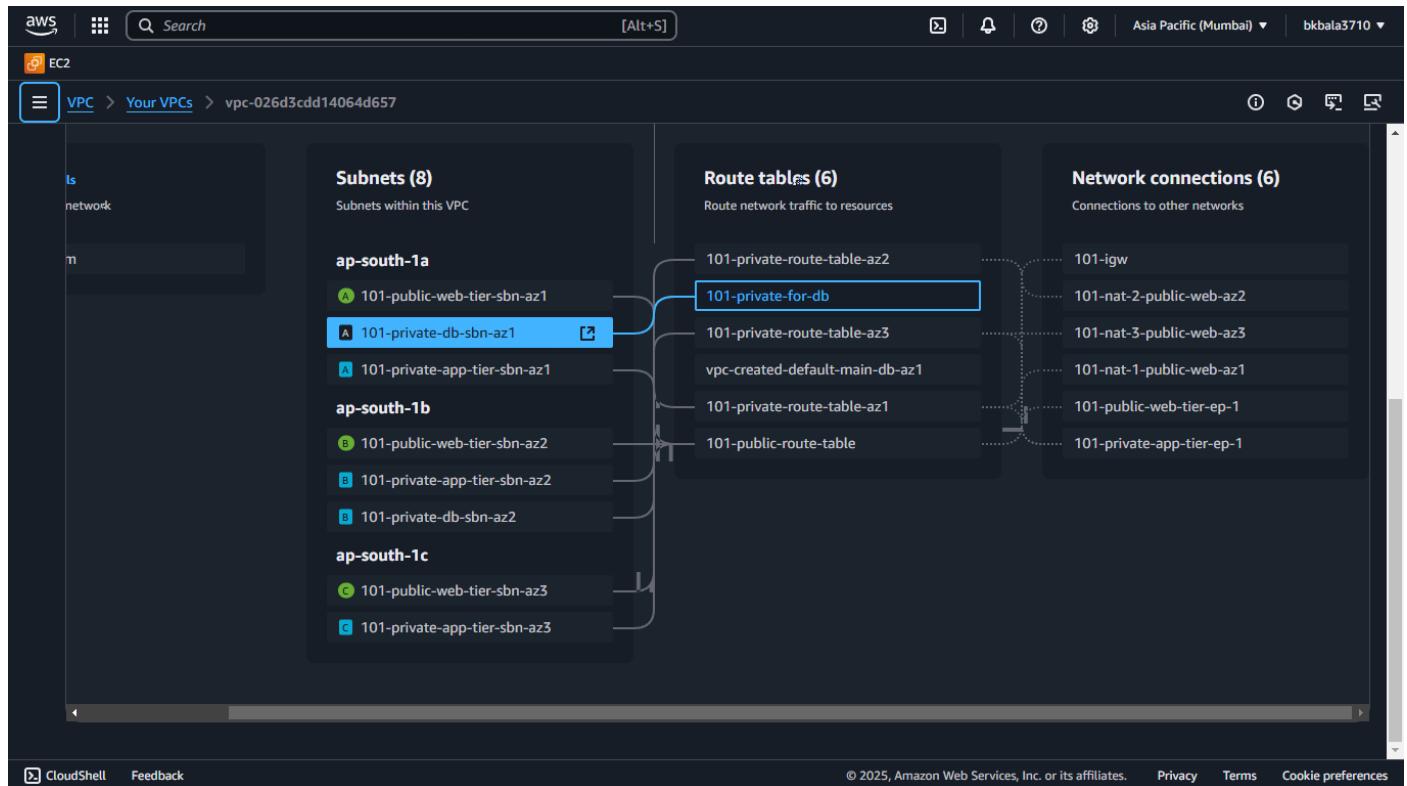
```
34. pm2 startup  
35. pm2 save  
36. curl http://localhost:4000/health
```

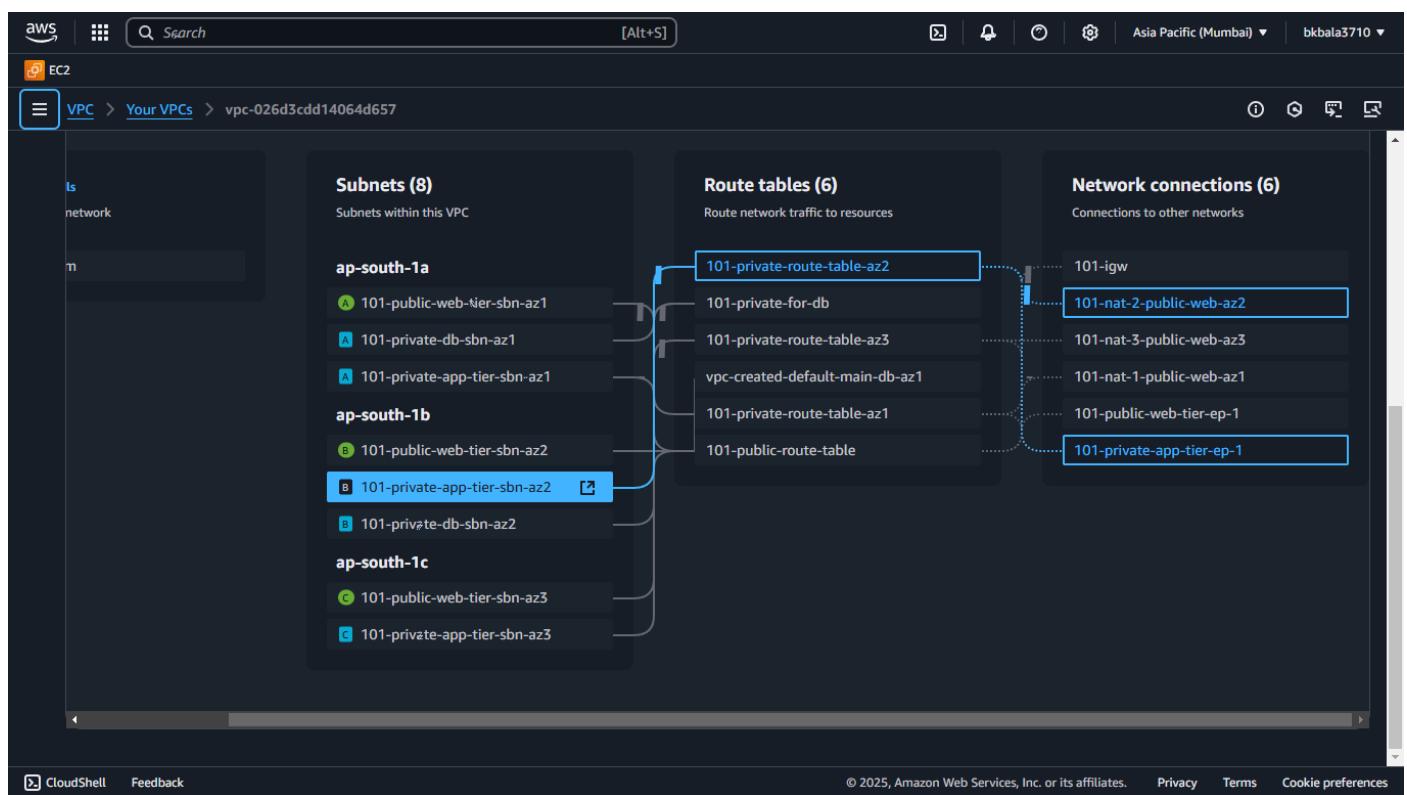
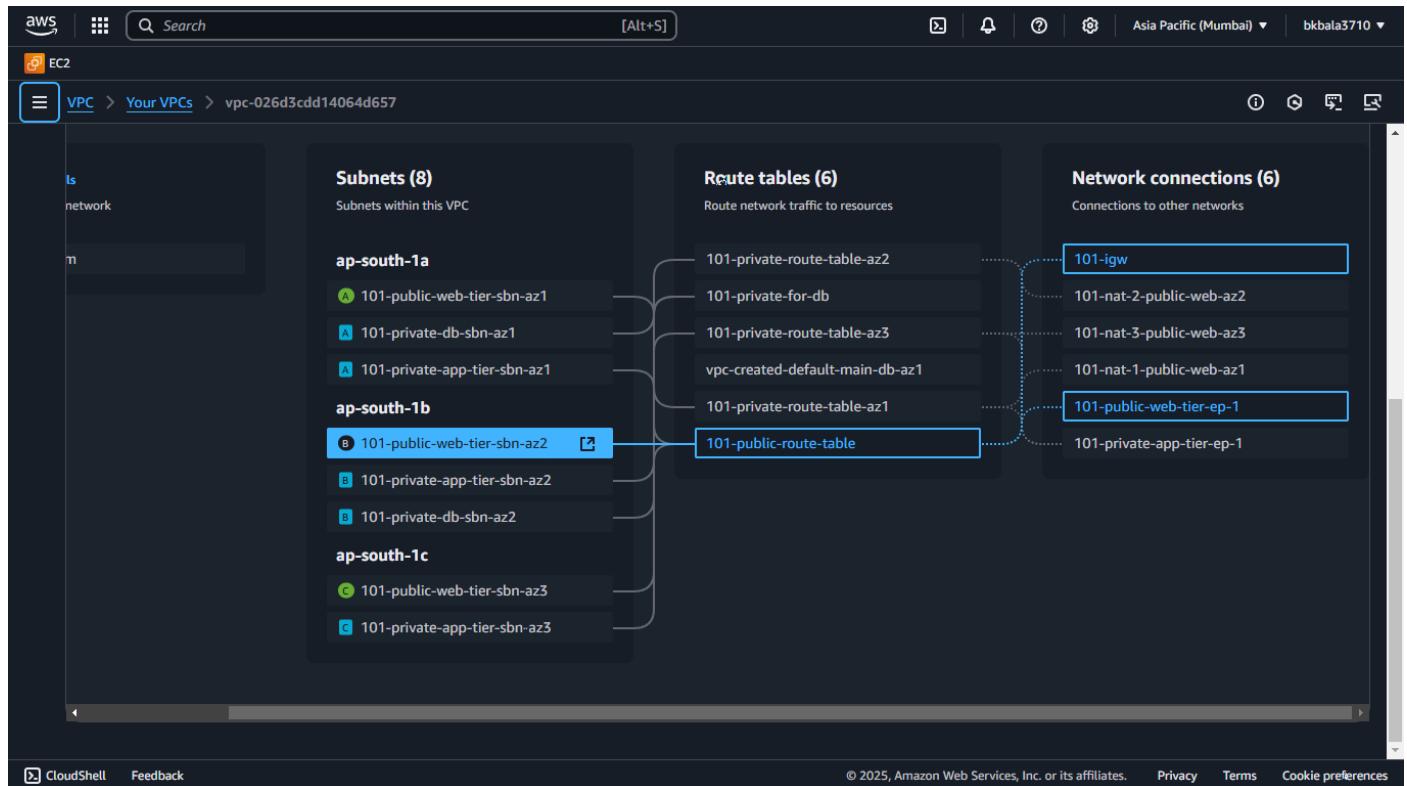
It should return: This is the health check.

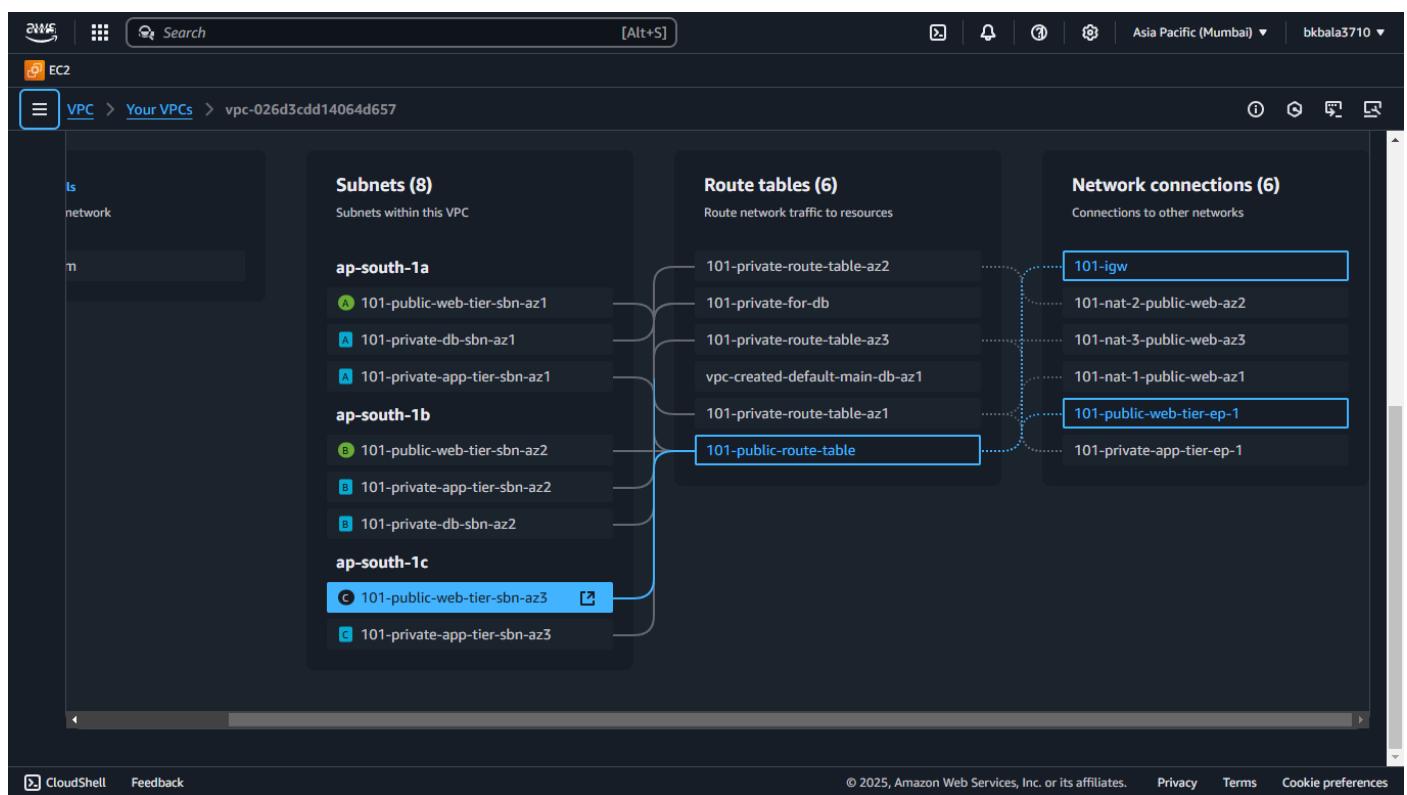
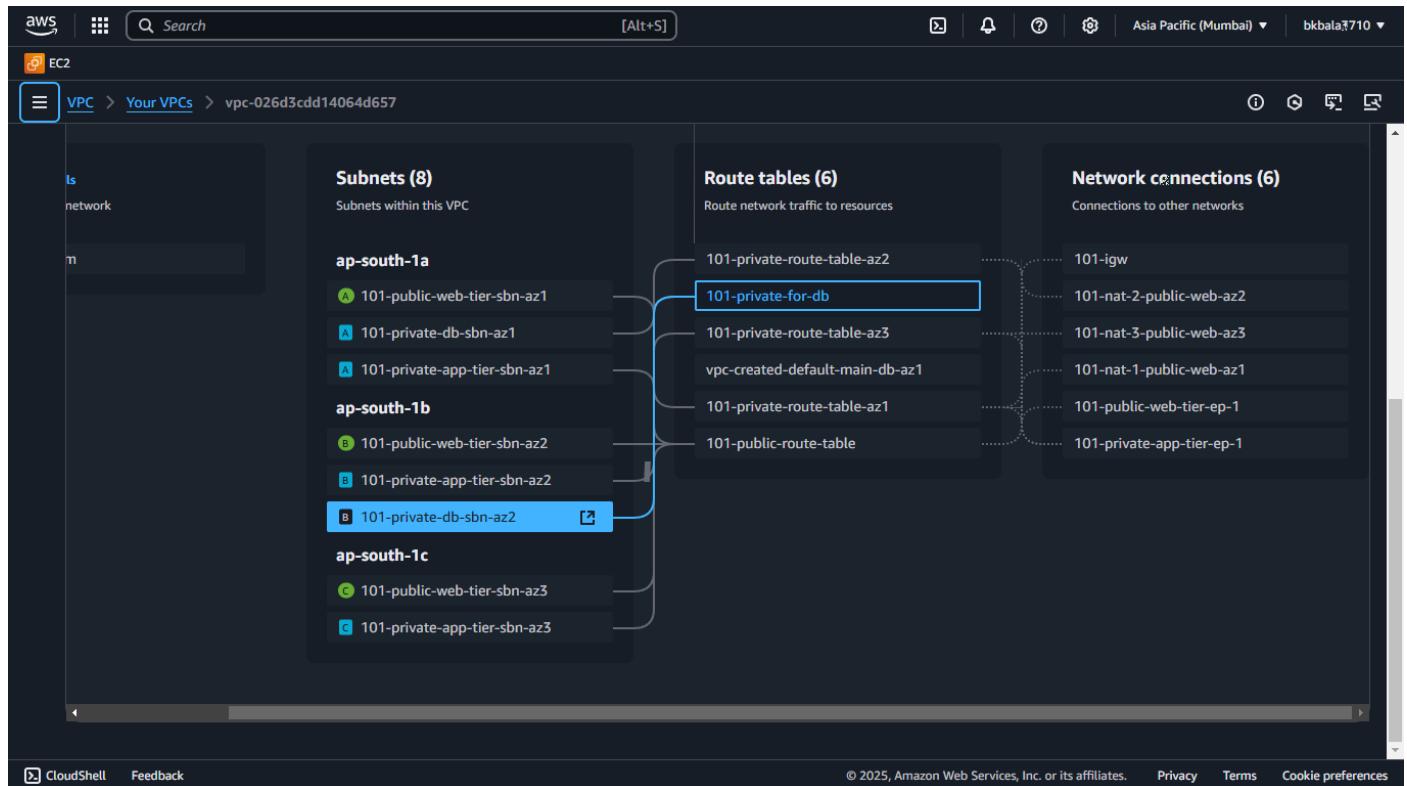
```
37. Creation of Internal Load Balancer for App Tier ec2 instance  
38. Update the nginx.conf file in S3 with internal load balancer DNS.  
39. Login to web tier ec2 via SSM system manager – connect (key not required – IAM)  
40. sudo -su ec2-user  
41. cd /home/ec2-user  
42. curl -o- https://raw.githubusercontent.com/avizway1/aws_3tier_architecture/main/ins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

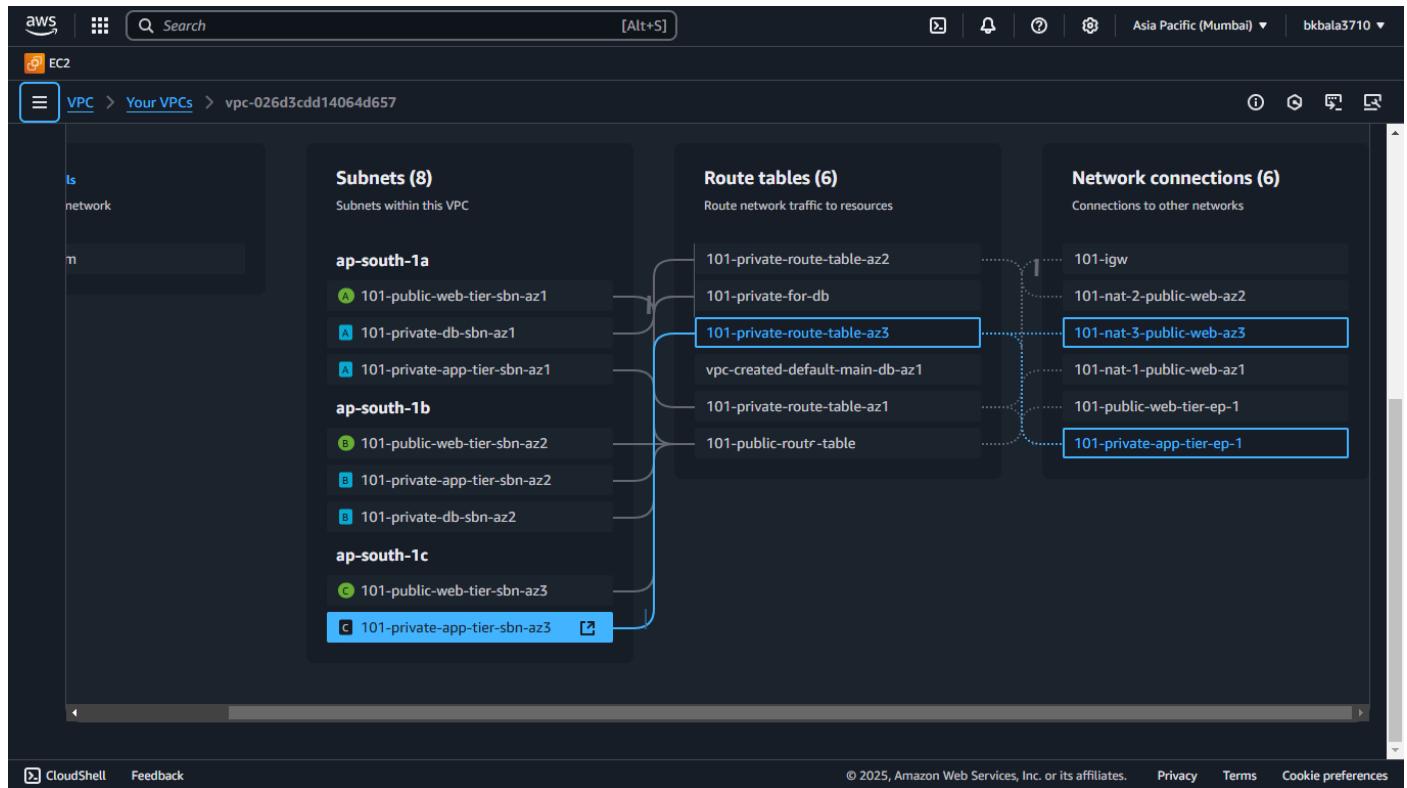
48. cd web-tier
49. npm install
50. npm run build
51. sudo amazon-linux-extras install nginx1 -y
52. cd /etc/nginx (You are in nginx path)
53. ls ----> You will see 'nginx.conf' file
54. sudo rm nginx.conf
55. sudo aws s3 cp s3://<S3 Bucket Name>/application-code/nginx.conf .  
Ex: sudo aws s3 cp s3://demo-3tier-project/application-code/nginx.conf .  
(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\\_auIKA&t=721s](https://www.youtube.com/watch?v=Oj-Hr_auIKA&t=721s)