Production-Grade Cloud Networking Project

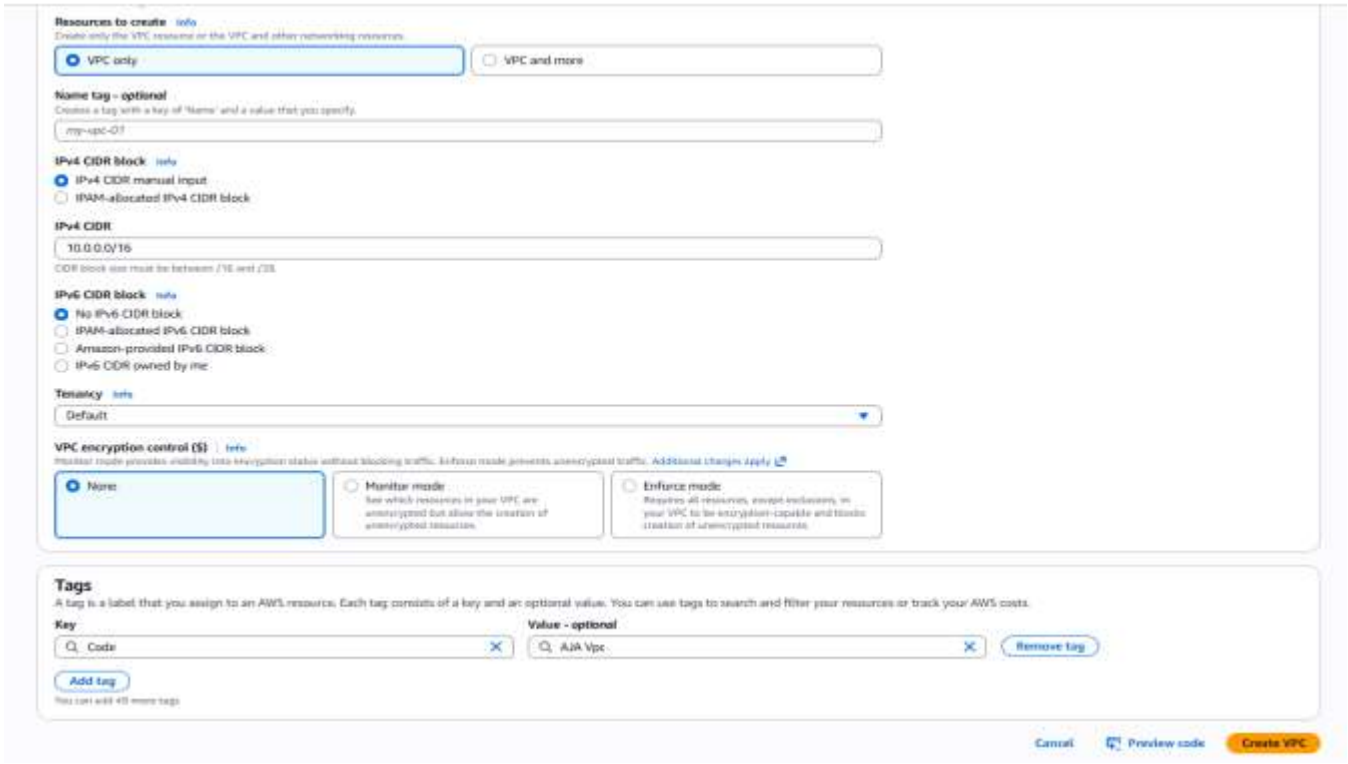
AWS VPC Design with Multi-Size Subnets & Controlled Internet Access

STEP 1: Steps to open **VPC** in AWS Console :

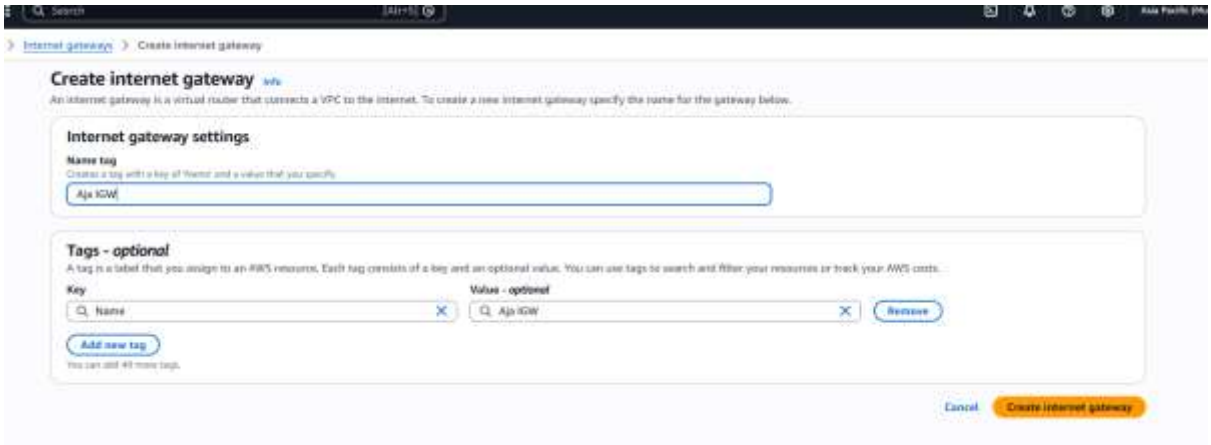
1. Login to **AWS** Console.
2. Make sure the region is **Asia Pacific (Mumbai)**.
3. In the search bar, type **VPC**.
4. Click on **VPC – Isolated Cloud Resources**.
5. You will be redirected to the **VPC Dashboard**.
6. From left menu you can create:
    - VPC
    - Subnets
    - Route Tables
    - Internet Gateway
    - NAT Gateway
    - Security Groups
    - NACLs

STEP 2: **create a VPC**, next steps:

1. Click **Create VPC**.
2. Select **VPC only**.
3. Enter CIDR (example: 10.0.0.0/16).
4. Click **Create VPC**.



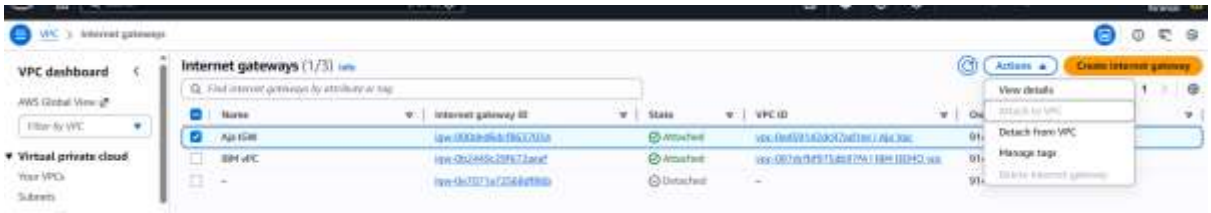
STEP 3: Create and attach an **Internet Gateway (IGW)** in AWS:



A. Create Internet Gateway

1. Go to **VPC Dashboard**.
2. Click **Internet Gateways** (left menu).
3. Click **Create internet gateway**.
4. Enter **Name tag** → Aja IGW
5. (Optional) Add tags.
6. Click **Create internet gateway**.

B. Attach Internet Gateway to VPC



7. Select the created IGW
8. Click **Actions** → **Attach to VPC**.
9. Choose your VPC (example: Aja-VPC or 10.0.0.0/16).
10. Click **Attach internet gateway**.

C. Add Route to Public Subnet

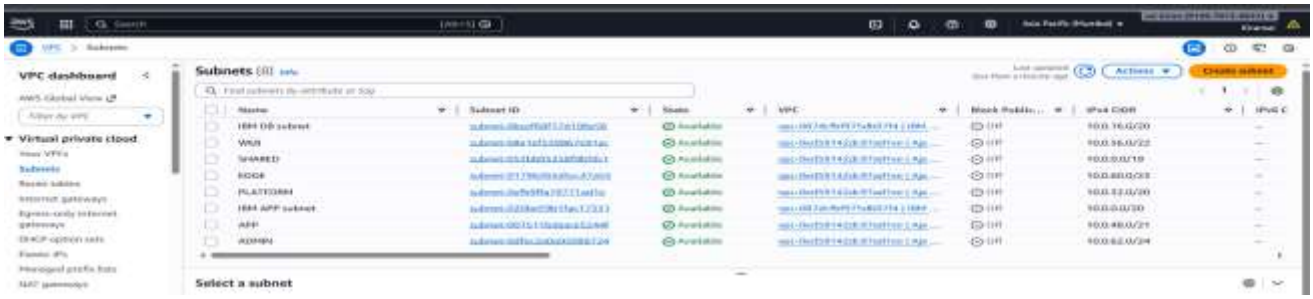
11. Go to **Route Tables**.
12. Select your **Public Route Table**.
13. Click **Edit routes** → **Add route**.
14. Destination: 0.0.0.0/0
15. Target: **Internet Gateway (Aja IGW)**.
16. Click **Save routes**.

Now your **public subnet has internet access**.

STEP 4: To create the **Subnet**

1. Go to **VPC Dashboard**.
2. Click **Subnets** → **Create subnet**.
3. Select your **VPC** (example: 10.0.0.0/16).
4. Under **Subnet 1 of 3**:
    - **Subnet name**: SHARED
    - **Availability Zone**: Select **No preference** (or choose ap-south-1a if needed)
    - **IPv4 VPC CIDR block**: 10.0.0.0/16
    - **IPv4 subnet CIDR block**: 10.0.0.0/19
      (This gives 8,192 IPs)
5. Tags (optional):
    - Key: Name
    - Value: SHARED
6. Click **Create subnet**.

If you are creating 6 subnets.



Subnet 1 of 3

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
SHARED
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
No preference

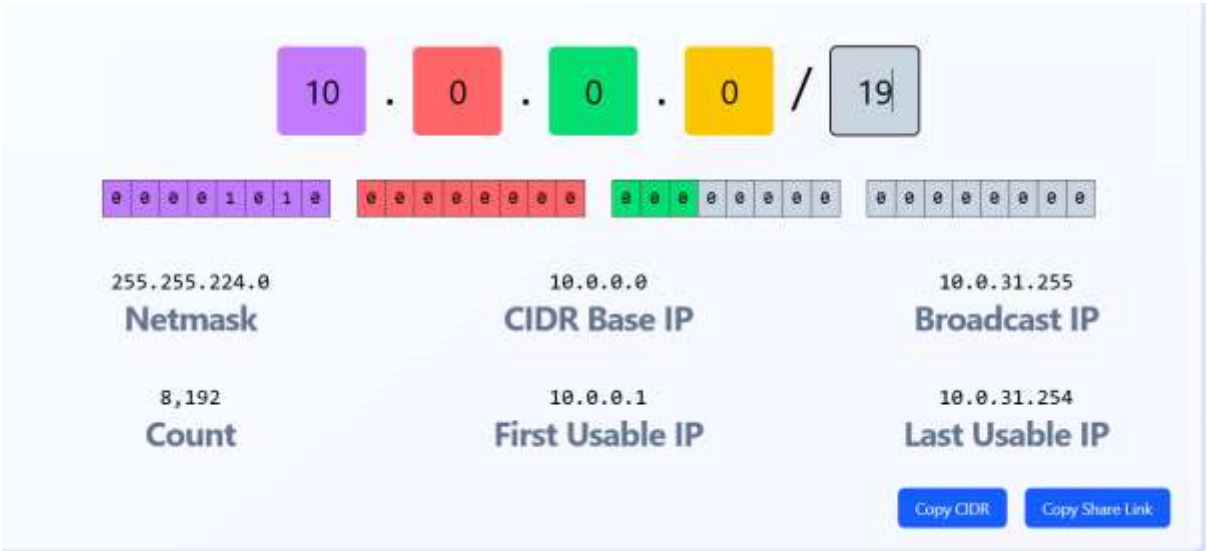
IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

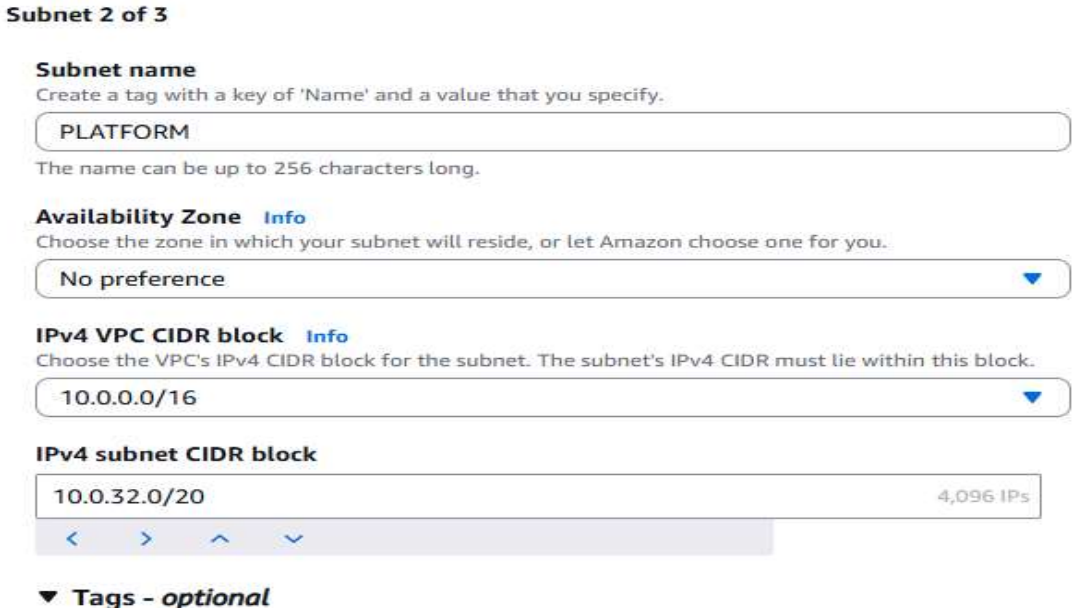
IPv4 subnet CIDR block
10.0.0.0/19 8,192 IPs

Tags - *optional*

Key	Value - *optional*	
Name	SHARED	Remove

Add new tag
You can add 49 more tags.
Remove



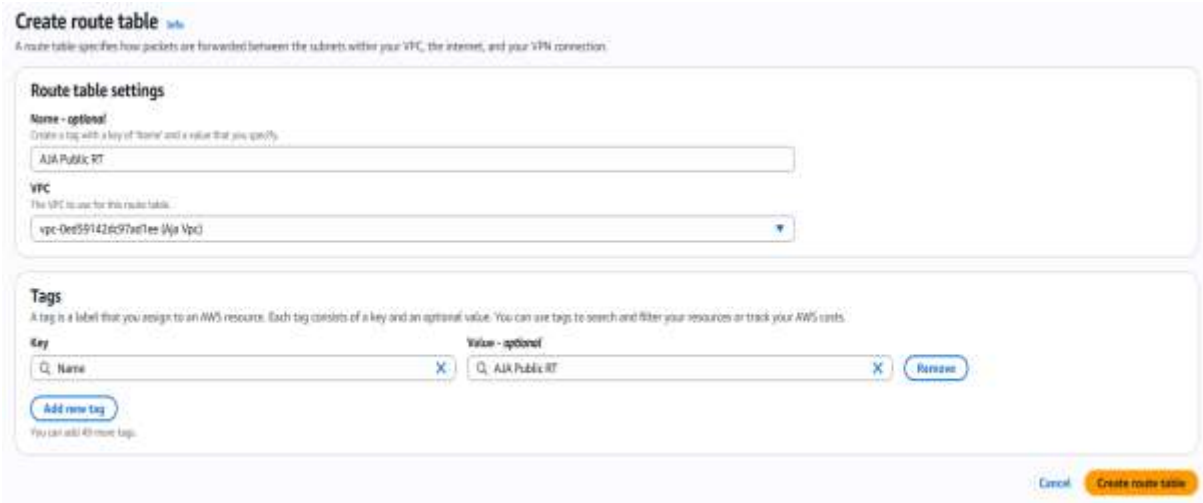


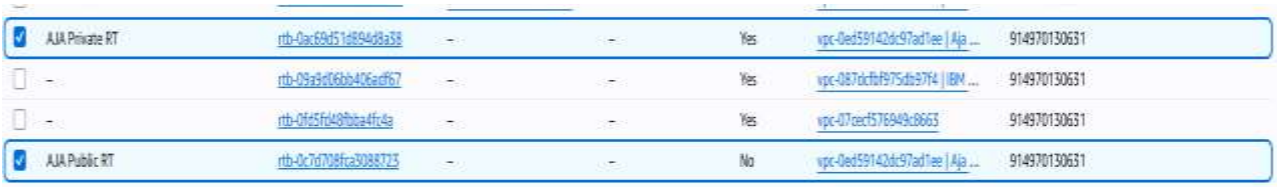
STEP 5 : Create **Route Table**

1. Go to **VPC Dashboard**.
2. Click **Route Tables** (left side).
3. Click **Create route table**.
4. In **Name**: AJA Public RT
5. Select **VPC**: Aja VPC (10.0.0.0/16)
6. Tags:
    - Key: Name
    - Value: AJA Public RT
7. Click **Create route table**.

B. Add Internet Route

8. Select the created route table (AJA Public RT).
9. Go to **Routes** tab → Click **Edit routes**.
10. Click **Add route**:
    - Destination: 0.0.0.0/0
    - Target: **Internet Gateway (Aja IGW)**
11. Click **Save routes**.

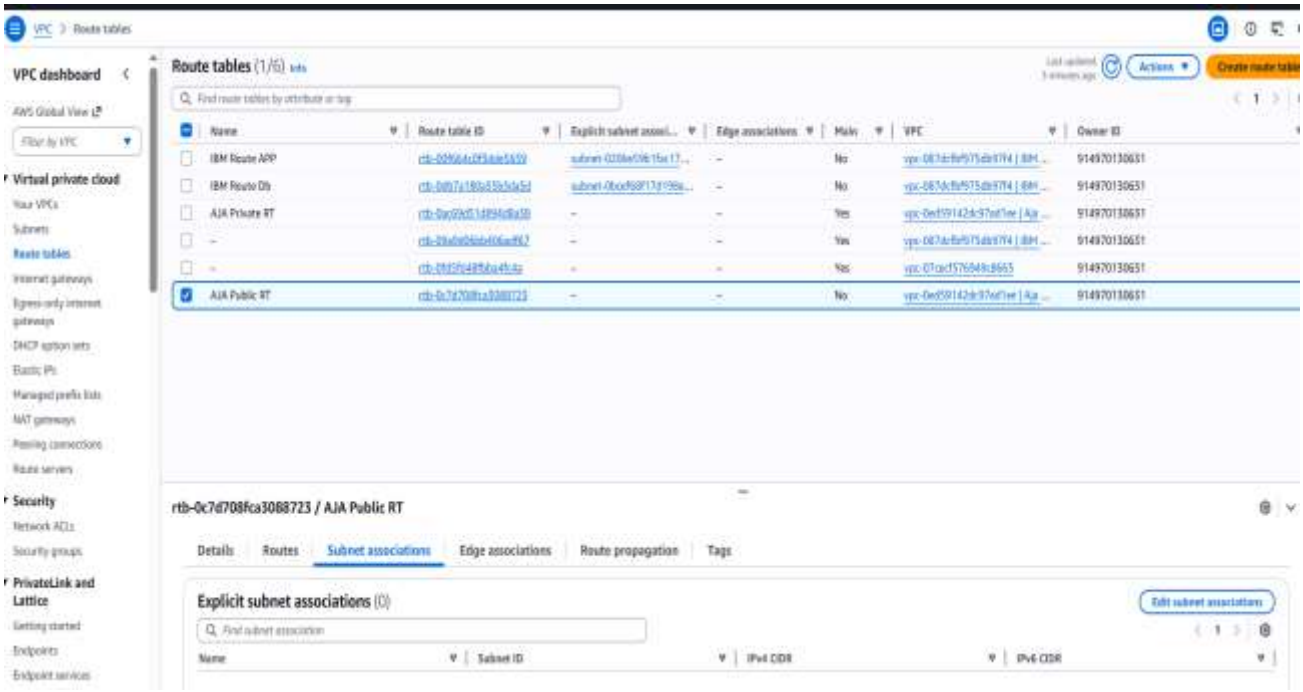


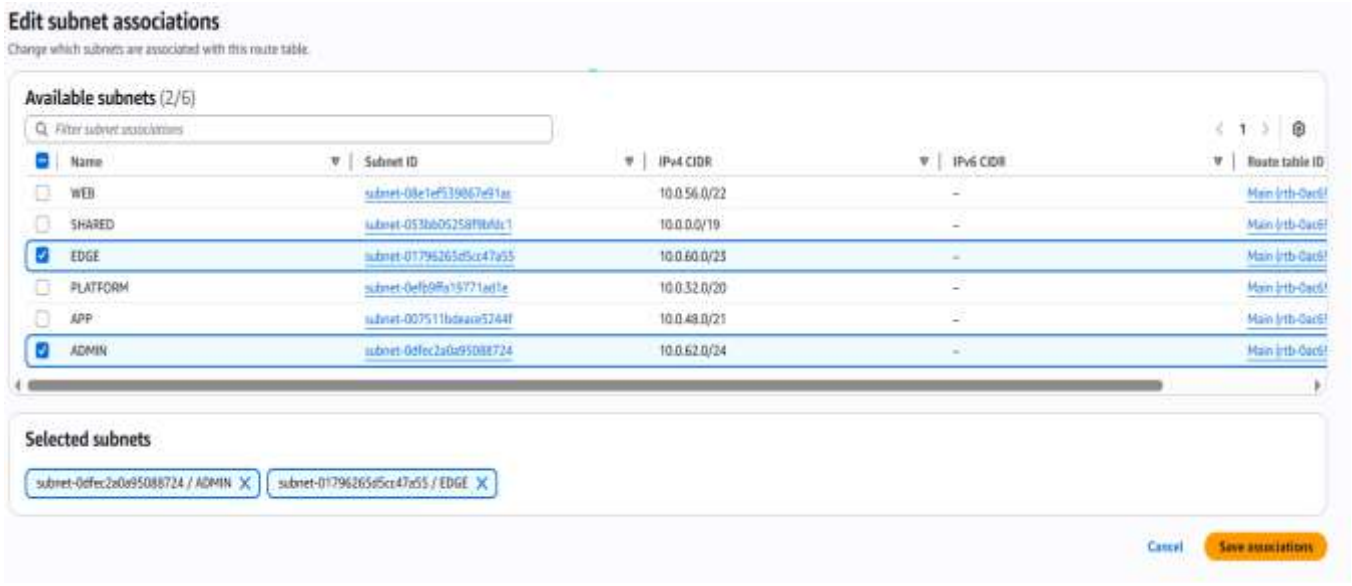


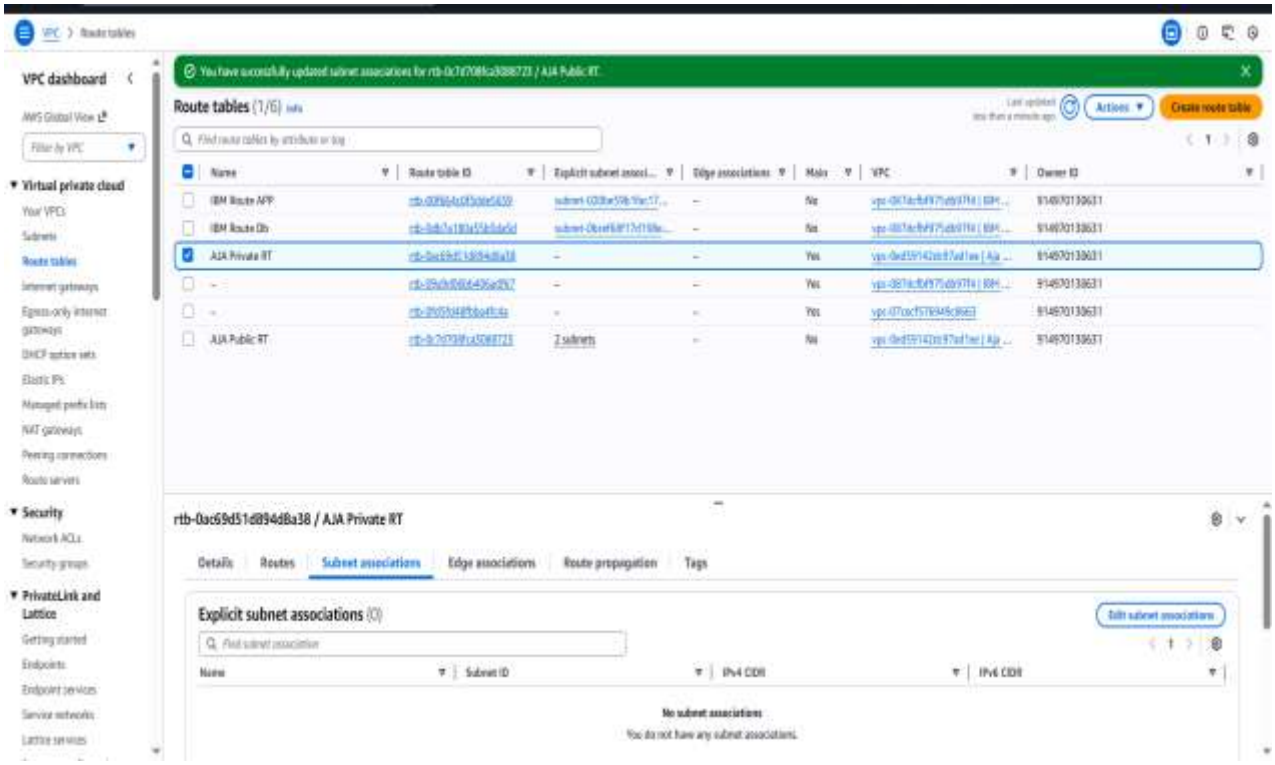
C. Associate with Public Subnet

12. Go to **Subnet associations** tab.
13. Click **Edit subnet associations**.
14. Select your **Public subnet**.
15. Click **Save associations**.

Now your public subnet can access the internet.


VPC dashboard
Route tables (1/6)
Name
Route table ID
Main
VPC
Owner ID
IBM Route APP
IBM Route DB
AJA Private RT
AJA Public RT
rtb-0c7d708fca3088723 / AJA Public RT
Details
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (0)
Edit subnet associations
Subnet ID
IPv4 CIDR
IPv6 CIDR


Edit subnet associations
Change which subnets are associated with this route table.
Available subnets (2/6)
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
Route table ID
WEB
SHARED
EDGE
PLATFORM
APP
ADMIN
Selected subnets
subnet-0dfec2a0a95088724 / ADMIN
subnet-01796265d5cc47a55 / EDGE
Cancel
Save associations



STEP 6: To add Internet Gateway route:

1. Go to **VPC Dashboard**
2. Click **Route Tables**
3. Select your route table
4. Click **Routes tab**
5. Click **Edit routes**

Now add this:

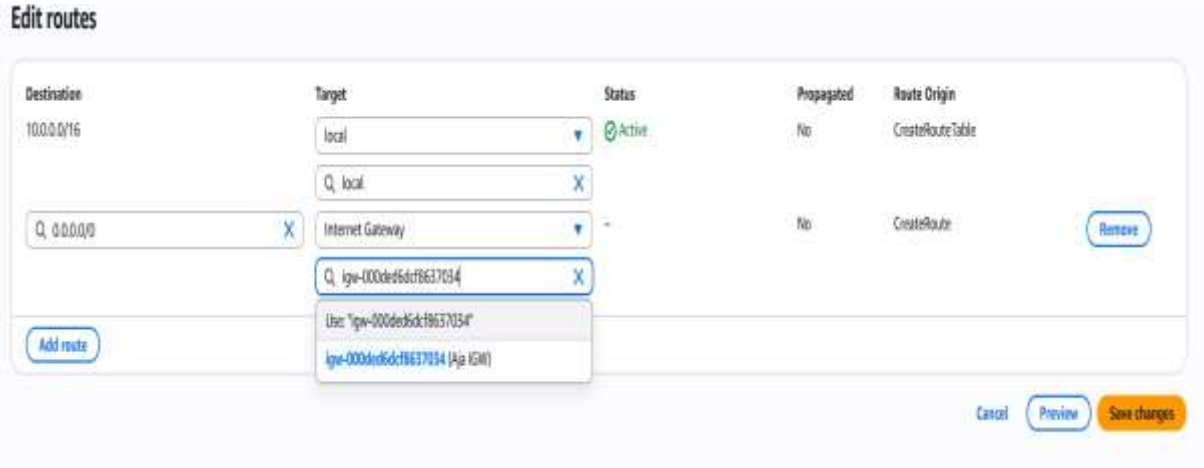
6. Click **Add route**
7. In **Destination** → enter 0.0.0.0/0
8. In **Target** → select **Internet Gateway (igw-xxxxxx)**

You will see:

- 10.0.0.0/16 → local (already there, don't change)
- 0.0.0.0/0 → igw-xxxxxx

9. Click **Save changes**

Now this subnet becomes **Public Subnet** (it has internet access).



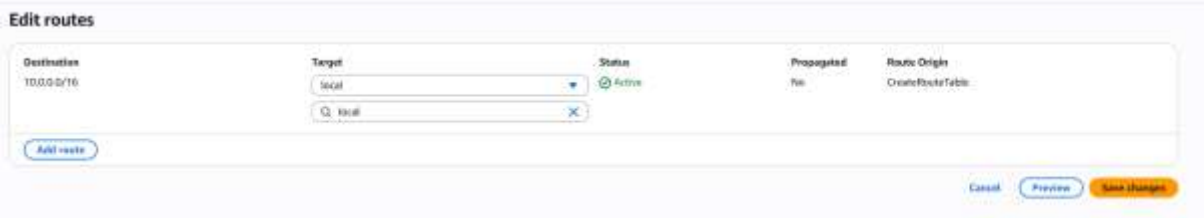
STEP 7: You are in **Route Table → Edit routes**.

Right now it has only one rule:

10.0.0.0/16 → local

This means:

- All computers (EC2) inside your VPC can talk to each other.
- They **cannot go to the internet** yet.

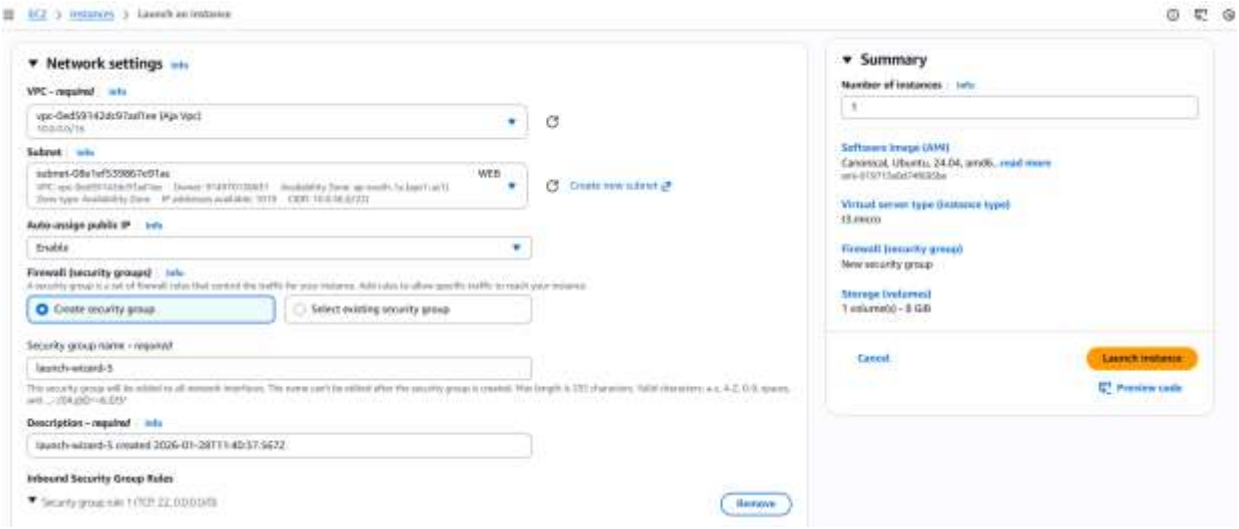


STEP 8: Instance creation for Validation and Testing

Simple steps to launch EC2 in your VPC:

1. Go to **EC2 → Instances → Launch instance**
2. Select **AMI**: Ubuntu 24.04
3. Select **Instance type**: t3.micro
4. In **Network settings**:
    - VPC: **Aja VPC (10.0.0.0/16)**
    - Subnet: **WEB (Public Subnet)**
    - Auto-assign Public IP: **Enable**

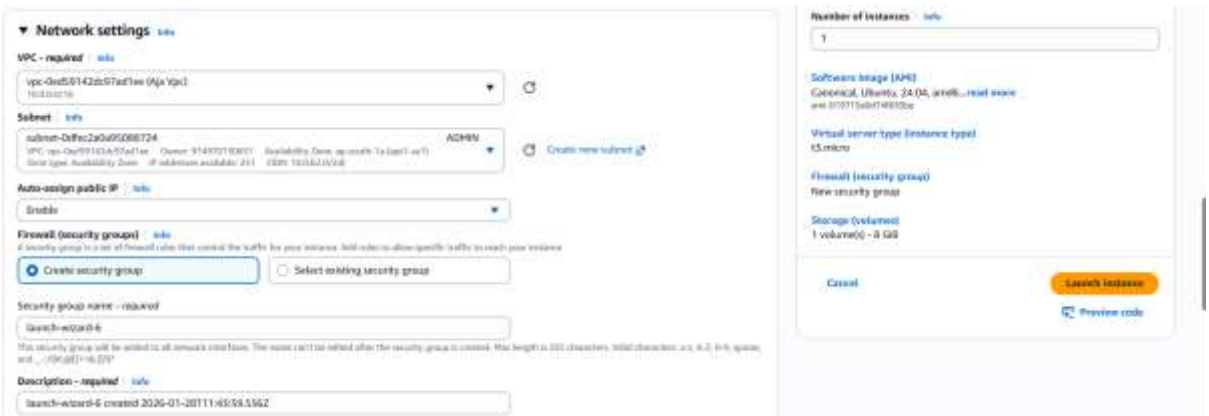
5. Create **Security Group**:
    - Allow **SSH (22)** from **0.0.0.0/0**
6. Select or create **Key Pair**
7. Click **Launch instance**



Private Subnet Validation

- EC2 instances in Web/App/Platform/Shared:
    - Cannot reach the internet
    - Can communicate internally

Why: No route to IGW exists



Public Subnet Validation

- **EC2 instances in Admin/Edge can:**
  - Resolve DNS
  - Reach external IPs
  - Access the internet

Why: Route table contains 0.0.0.0/0 → IGW