Step-by-Step Implementation

> by Shloka Kamdar

Step 1: Set up the virtual private cloud

1. **Create VPC**
   - **Name:** vpc-shloka-nginx
   - **Region:** us-west-2 (Oregon)
   - **CIDR:** 10.0.0.0/16

     Reason: Provides an isolated networking environment for secure infrastructure.
2. **Create Subnets (Minimum 2 for HA)**
   - **private-subnet-01-shloka-nginx:** 10.0.1.0/24 (us-west-2a)
   - **public-subnet-01-shloka-nginx:** 10.0.2.0/24 (us-west-2a)
   - **private-subnet-02-shloka-nginx :** 10.0.3.0/24 (us-west-2b)
   - **public-subnet-02-shloka-nginx:** 10.0.4.0/24 (us-west-2b)

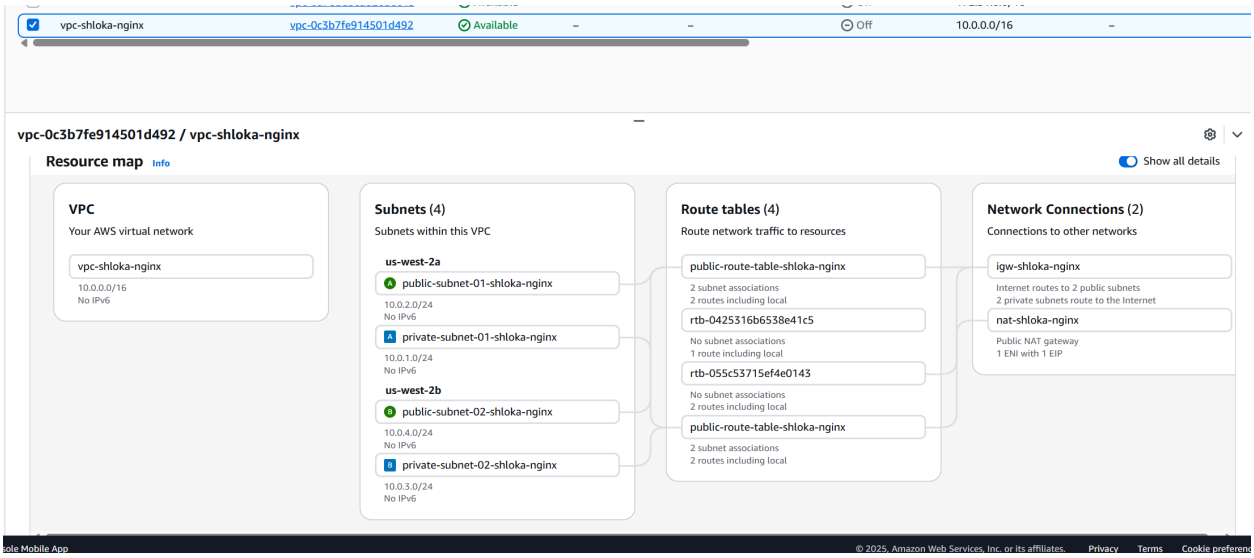
   Reason: Separate public-facing resources from private application servers.
3. **Create IGW Gateway**
   - **IGW Name:** igw-shloka-nginx
   - Attached to VPC

   Reason: Allows internet traffic for ALB and Bastion.
4. **Create NAT Gateway**
   - Created a NAT Gateway: **nat-shloka-nginx**
   - **Reason:** Private EC2 could not install packages → user-data failed. NAT fixed this.
5. **Create Route Tables**

- **Public Route Table:** public-route-table-shloka-nginx
  - 0.0.0.0/0 → Internet Gateway
- **Private Route Table:** private-route-table-shloka-nginx
  - 0.0.0.0/0 → NAT Gateway

Reason: Ensures public resources get internet and private resources get outbound access through NAT.

Resource Map —



Step 2: Launch EC2 Instances

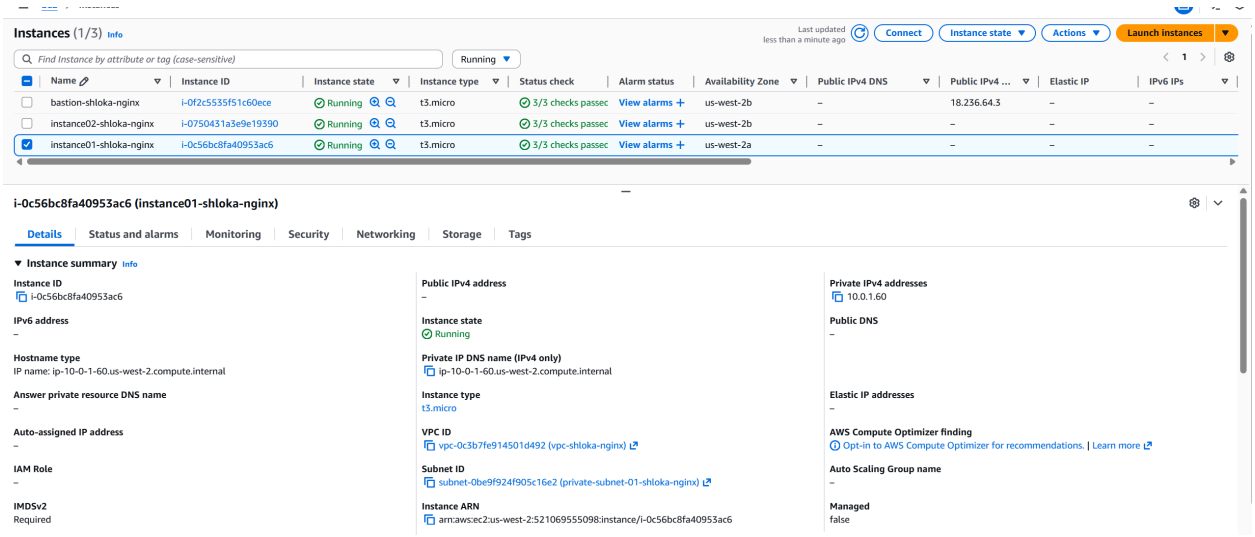
1. **2 Private EC2 instances** (for application) in different subnets
   - **instance02-shloka-nginx** - private subnet A
   - **instance01-shloka-nginx** - private subnet B

User Data Script :

```
#!/bin/bash
sudo apt update -y
sudo apt install -y nginx
```

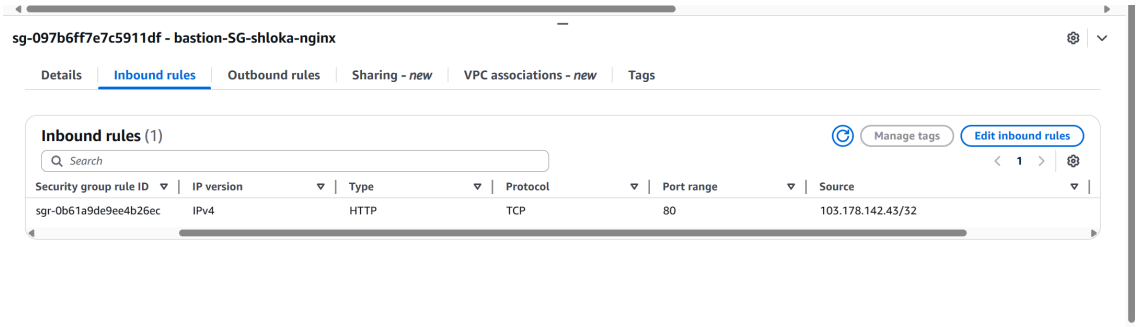
```
sudo sed -i 's/listen 80 default_server;/listen 8443 default_server;/' /etc/nginx/sites-available/default
sudo sed -i 's/listen \[::\]:80 default_server;/listen \[::\]:8443 default_server;/' /etc/nginx/sites-available/default

echo "<h1>Shloka — ALB Test on Port 8443</h1>" | sudo tee /var/www/html/index.html

sudo systemctl enable nginx
sudo systemctl restart nginx
```

2. **A Bastion Instance to SSH into other instances in private subnet**
    - **bastion-shloka-nginx** - public subnet A

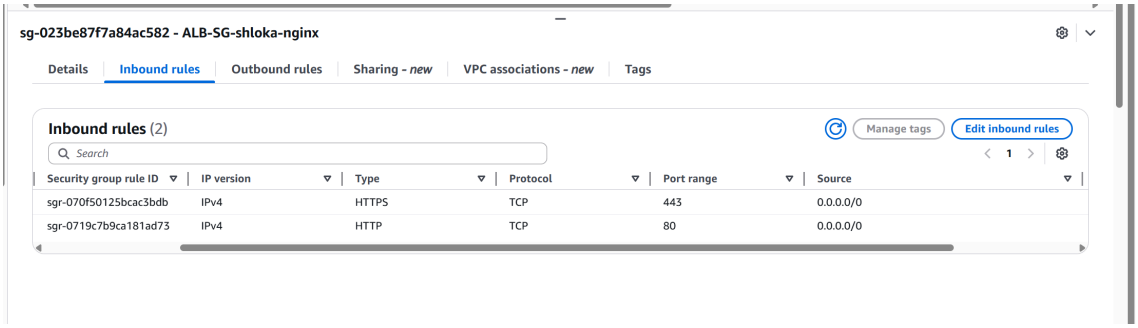


Step 3: Configure Security Groups

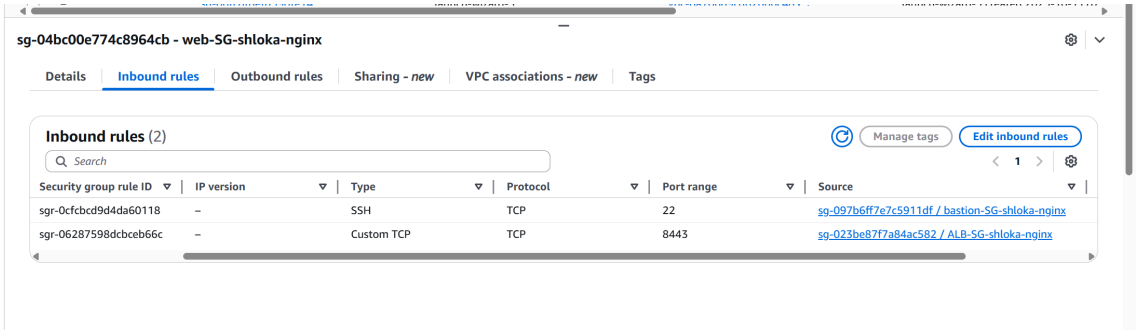
1. **Bastion SG:**
    - SSH (22): My IP only



2. **ALB SG:**
    - HTTP (80): 0.0.0.0/0
    - HTTPS (443): 0.0.0.0/0

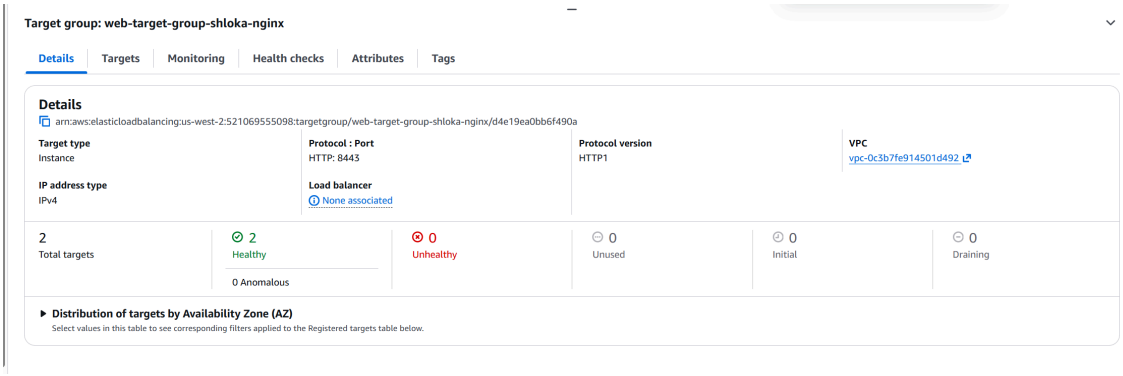


3. **Private EC2 SG:**
    - Allow 8443 **only from ALB SG**
    - Allow SSH **only from Bastion SG**

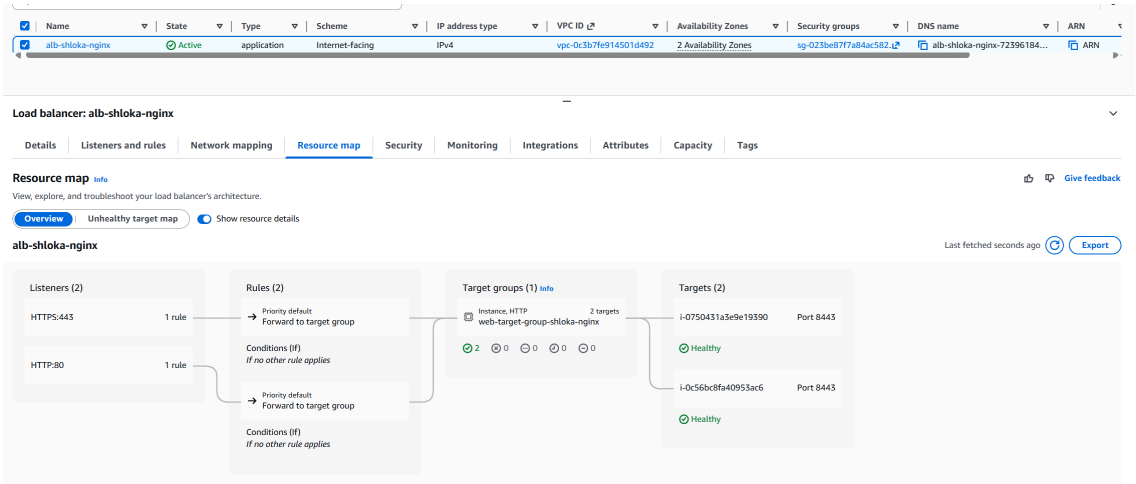


Step 3: Create Target Group & Load Balancer

- **Target Group**
  - Listens on Port 8443
  - Associated with 2 instances (application servers)



2. ALB
   - In both the public subnets
   - Listener: 80 → forward to TG
   - Later updated to 443 for HTTPS

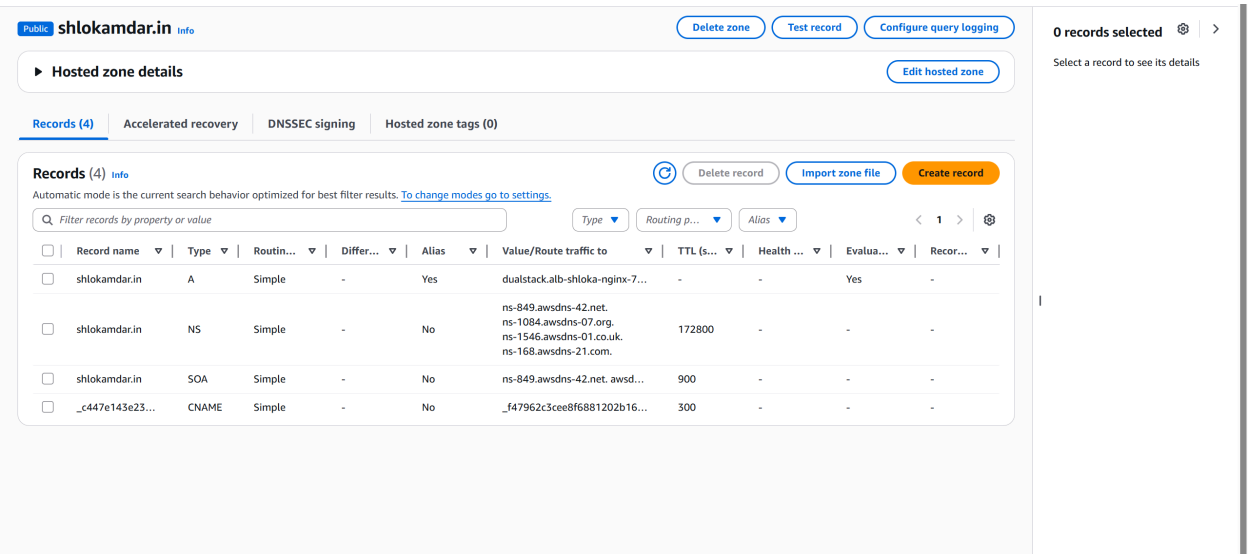


Step 4: Configure Route 53 DNS

- Updated GoDaddy nameservers to Route 53's nameservers

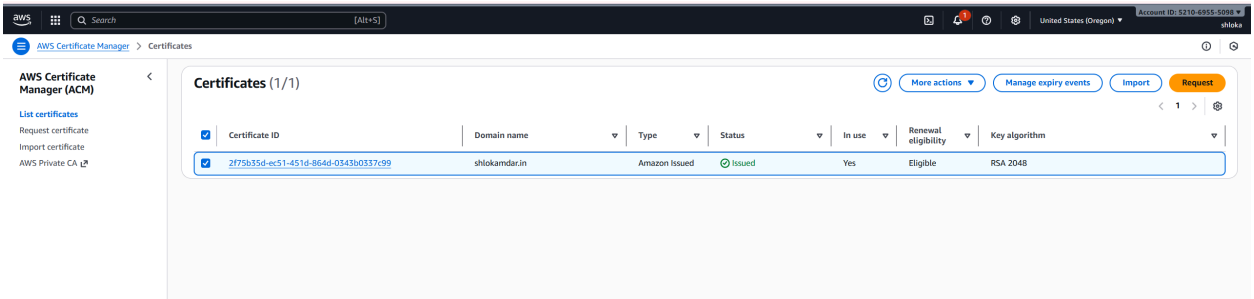
- Created Hosted Zone in route 53
- Created A (Alias) record to ALB's DNS record

  Reason: Required for domain → ALB routing.



Step 5: HTTPS Setup (ACM Certificate)

- Requested certificate for:
  - shlokamdar.in



- DNS validation (took time due to propagation)
- Attached certificate to ALB Listener on port 443

  Result → **Secure HTTPS website working**