web-application

Deploy a simple web application on AWS that demonstrates your understanding of cloud infrastructure, networking, and basic DevOps practices.

Architecture Overview

This project deploys a highly available web application using AWS services. Traffic is routed through an Application Load Balancer (ALB) to EC2 instances running in private subnets across multiple Availability Zones.

Key design highlights:

1. Multi-AZ architecture
2. Public and private subnet separation
3. Secure access using security groups
4. Outbound internet access via NAT Gateway

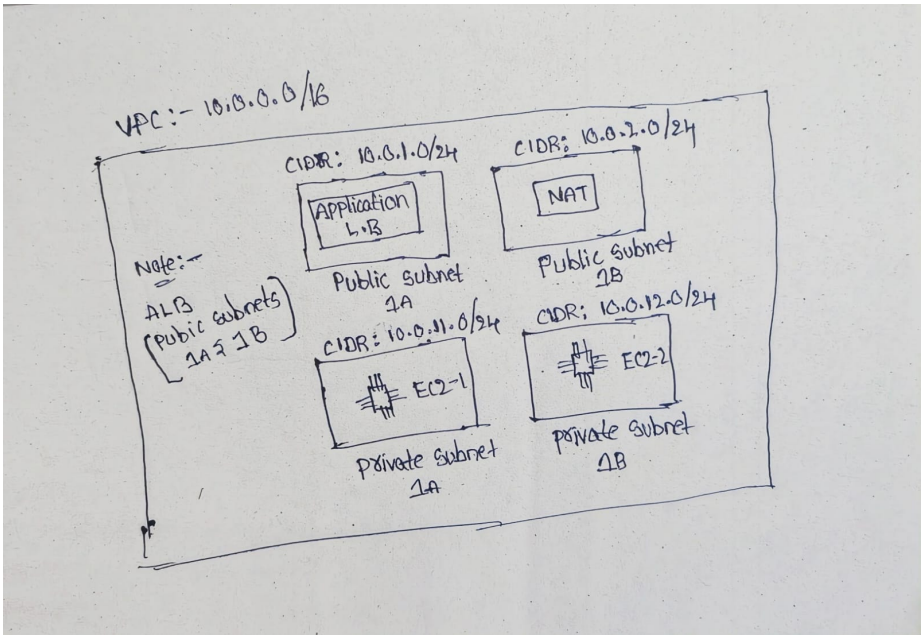

Figure 1: WhatsApp Image 2026-02-05 at 10 08 29 PM (1)

AWS Resources Used

Networking

1. VPC (10.0.0.0/16)

2. Public Subnets (AZ 1A, 1B)
3. Private Subnets (AZ 1A, 1B)
4. Internet Gateway
5. NAT Gateway
6. Public and Private Route Tables
7. Elastic IP

Compute & Load Balancing

1. Two EC2 Instances (Amazon Linux)
2. Application Load Balancer
3. Target Group

Security

1. Security Group for ALB
2. Security Group for EC2 instances

Step-by-Step Implementation

1. VPC and Subnets

1. Created a VPC with CIDR 10.0.0.0/16
2. Created public and private subnets across two Availability Zones

2. Internet & NAT Access

1. Attached Internet Gateway to VPC
2. Configured public route table for internet access
3. Deployed NAT Gateway in a public subnet
4. Associated private subnets with NAT Gateway for outbound access

3. EC2 Setup

1. Launched EC2 instances in private subnets
2. Installed and configured Nginx
3. Deployed a sample webpage displaying: Instance ID Availability Zone Served by Nginx

4. Application Load Balancer

1. Created ALB in public subnets
2. Configured listener on port 80
3. Registered EC2 instances in target group
4. Enabled health checks
5. Health checks configured on path `/` using HTTP

5. Validation

1. Accessed application using ALB DNS name
2. Confirmed successful response
3. Verified load distribution between EC2 instances Instance 1

instance 2

Security Group Configuration

- EC2 instances do not have public IPs
- EC2 instances are not directly accessible from the internet
- All inbound traffic to EC2 flows only through the Application Load Balancer
- NAT Gateway is used only for outbound internet access (package updates, installs)

ALB Security Group

1. Inbound: HTTP (80) from 0.0.0.0/0
2. Outbound: All traffic allowed

EC2 Security Group

1. Inbound: HTTP (80) from ALB Security Group only
2. Outbound: All traffic allowed via NAT Gateway

Configuration Files

EC2 User Data Script

The EC2 instances are configured using a user data script during launch.
This script installs and configures Nginx, retrieves instance metadata securely using IMDSv2, and dynamically generates a custom HTML page.

User Data Script

“‘bash #!/bin/bash dnf update -y dnf install nginx -y systemctl enable nginx systemctl start nginx

TOKEN=$(curl -X PUT “http://169.254.169.254/latest/api/token”
-H “X-aws-ec2-metadata-token-ttl-seconds: 21600”)

INSTANCE_ID=$(curl -H “X-aws-ec2-metadata-token: $TOKEN”
http://169.254.169.254/latest/meta-data/instance-id)

AZ=$(curl -H “X-aws-ec2-metadata-token: $TOKEN”
http://169.254.169.254/latest/meta-data/placement/availability-zone)

cat < /usr/share/nginx/html/index.html <!DOCTYPE html>

Hello World

Hello World!

Instance ID: $INSTANCE_ID < /strong >< /p >< p > Availability Zone :< strong >$AZ

Served by: Nginx

EOF