3 Tier Web Architecture – VPC & Networking Documentation

1. Overview

This document describes the **updated VPC and networking setup** for our **3 Tier Web Architecture Project** after migrating the infrastructure to **AWS Region: US East (N. Virginia – us-east-1)**.

The migration was done primarily for **cost optimization**, better service availability, and alignment with common production best practices.

The scope of this document covers:

- VPC creation
- Subnet design across Availability Zones
- Route table strategy
- Internet Gateway configuration

---

2. Region & Availability Zones

- **AWS Region:** us-east-1 (N. Virginia)
- **Availability Zones Used:**
    - us-east-1c (AZ1)
    - us-east-1d (AZ2)

The architecture is deployed across **two AZs** to ensure **high availability and fault tolerance**.

---

3. VPC Configuration

- **VPC Name:** prod-vpc-3tier
- **CIDR Block:** 10.0.0.0/16
- **Total IP Addresses:** 65,536

The /16 CIDR range provides sufficient IP capacity for current workloads and future expansion.

---

4. Subnet Architecture (6 Subnets)

We created **6 subnets**, evenly distributed across two Availability Zones.

4.1 Subnets in us-east-1c (AZ1)

1. **Public Subnet (Web Tier / ALB)**

    - Name: prod-public-subnet-alb-az1-web-tier
    - CIDR: 10.0.0.0/20

2. **Private Subnet (Application Tier)**
    - Name: prod-private-subnet-az1-app-tier
    - CIDR: 10.0.32.0/20
3. **Private Subnet (Database Tier)**
    - Name: prod-private-subnet-az1-db-tier
    - CIDR: 10.0.64.0/20

4.2 Subnets in us-east-1d (AZ2)

4. **Public Subnet (Web Tier / ALB)**
    - Name: prod-public-subnet-alb-az2-web-tier
    - CIDR: 10.0.16.0/20
5. **Private Subnet (Application Tier)**
    - Name: prod-private-subnet-az2-app-tier
    - CIDR: 10.0.48.0/20
6. **Private Subnet (Database Tier)**
    - Name: prod-private-subnet-az2-db-tier
    - CIDR: 10.0.80.0/20

4.3 Subnet Design Rationale

- **Public subnets** are used only for **external-facing components** (Load Balancer).
- **Application and Database tiers** are placed in **private subnets** for security.
- Each tier is spread across **two AZs** to avoid single points of failure.

---

5. Route Table Design (3 Route Tables)

We implemented **tier-based route tables** to maintain clean traffic separation and security boundaries.

5.1 Public Route Table (Web Tier)

- **Route Table Name:** 3-tier-public-RT
- **Associated Subnets:**

    - prod-public-subnet-alb-az1-web-tier
    - prod-public-subnet-alb-az2-web-tier

Routes:

- 10.0.0.0/16 → Local
- 0.0.0.0/0 → Internet Gateway

Purpose:
Allows inbound and outbound internet access for the external load balancer.

5.2 Private Route Table – Application Tier

- **Route Table Name:** 3-tier-private-RT-AZ1 / AZ2 (App Tier)
- **Associated Subnets:**
    - prod-private-subnet-az1-app-tier
    - prod-private-subnet-az2-app-tier

Routes:

- 10.0.0.0/16 → Local

Purpose:
Ensures application servers are **not directly exposed to the internet** and can communicate only within the VPC.

5.3 Private Route Table – Database Tier

- **Route Table Name:** 3-tier-private-RT-AZ1 / AZ2 (DB Tier)
- **Associated Subnets:**
    - prod-private-subnet-az1-db-tier
    - prod-private-subnet-az2-db-tier

Routes:

- 10.0.0.0/16 → Local

Purpose:
Provides maximum isolation for the database layer with **no internet access**.

---

6. Internet Gateway Configuration

- **Internet Gateway Name:** prod-igw
- **Attached To:** prod-vpc-3tier

The Internet Gateway is:

- Used **only by public subnets** via the public route table
- Required for external client access to the load balancer

Private subnets do **not** have direct routes to the Internet Gateway.

---

7. High-Level Traffic Flow

1. User requests enter via the **Internet Gateway**
2. Traffic reaches the **Load Balancer in public subnets**
3. Requests are forwarded to the **Application Tier in private subnets**
4. Application tier communicates with the **Database Tier** internally

This ensures a **secure, scalable, and production-ready architecture**.

---

8. Summary

- 1 VPC created with /16 CIDR
- 6 subnets across 2 AZs (public + private)
- 3 route tables aligned with tier-based design
- 1 Internet Gateway attached to the VPC
- Architecture optimized for **cost, security, and high availability**