# AWS 3-Tier Architecture with Bastion Host (Without Load Balancer)

## 1. VPC Creation

- Name: 3tier-vpc

- CIDR Block: 10.0.0.0/16

- DNS Hostnames and DNS Resolution: Enabled

## 2. Subnets Creation

Layer | Subnet Name | AZ | CIDR | Public/Private

---|---|---|---|---

Web Tier | Public-Subnet-A | us-east-1a | 10.0.1.0/24 | Public

Web Tier | Public-Subnet-B | us-east-1b | 10.0.2.0/24 | Public

Bastion Host | Bastion-Subnet | us-east-1a | 10.0.3.0/24 | Public

App Tier | Private-App-Subnet-A | us-east-1a | 10.0.11.0/24 | Private

App Tier | Private-App-Subnet-B | us-east-1b | 10.0.12.0/24 | Private

DB Tier | Private-DB-Subnet-A | us-east-1a | 10.0.21.0/24 | Private

DB Tier | Private-DB-Subnet-B | us-east-1b | 10.0.22.0/24 | Private

## 3. Internet Gateway (IGW)

- Create and attach IGW named '3tier-igw' to '3tier-vpc'.

## 4. Route Tables

- Public Route Table:

- Route 0.0.0.0/0 to IGW.

- Associate with Public and Bastion Subnets.

- Private Route Table for App Tier:

- Route 0.0.0.0/0 via NAT Gateway.

- Private Route Table for DB Tier:

- No external route.

## 5. NAT Gateways

- Create Elastic IPs.

- Create two NAT Gateways.

- Update App Tier Private Route Table.

## 6. Bastion Host Setup

- Deploy EC2 instance in Bastion-Subnet.

- Assign Public IP.

- SSH access only from Admin IP.

## 7. Web Tier EC2 Instances

- Deploy in Public-Subnet-A and B.

- Allow HTTP from Anywhere, SSH from Bastion Host.

## 8. App Tier EC2 Instances

- Deploy in Private-App-Subnets.

- Application access from Web Tier, SSH from Bastion Host.

## 9. Database Tier (RDS)

- Deploy RDS in Private-DB-Subnets.

- Access only from App Tier SG.

## 10. Security Groups Summary

SG Name | Allowed Inbound | Notes

---|---|---

Bastion SG | SSH (22) from Admin IP | Access to Bastion Host

Web Tier SG | HTTP (80) from Anywhere, SSH (22) from Bastion Host | Web Access

App Tier SG | App Port (8080) from Web Tier SG, SSH (22) from Bastion SG | Internal Traffic

DB Tier SG | DB Port (3306) from App Tier SG | Private Database Access

## 11. Traffic Flow

Internet → Bastion Host → Web EC2 → App EC2 → RDS

## 12. Notes

- Bastion Host for secured SSH.

- Private Subnets hidden from internet.

- Highly Available setup across AZs.