AWS Three-Tier Architecture Deployment with Terraform

## Architecture Layers:

1. **Web Tier** – Public-facing, handles incoming HTTP/HTTPS requests via a **Public ALB**.
2. **App Tier** – Internal application logic, accessible only via an **Internal ALB** from the Web tier.
3. **Database Tier** – Private **RDS MySQL** for persistent storage.

## Key Features:

* Infrastructure fully automated with Terraform
* Multi-AZ deployment for HA (High Availability)
* Auto Scaling Groups for web and app tiers
* Secure networking with private subnets & SG rules
* Centralized static file hosting in S3
* Parameter Store for DB credentials & endpoints

## Architecture Diagram

A diagram of a computer program

AI-generated content may be incorrect.

# Implementation Steps

## Phase 1: Defining variables and dependencies

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

## Phase 2: Custom VPC Creation

Provisioned a **custom VPC** with a CIDR block (e.g., 10.0.0.0/16) to host all resources.  
The VPC provides:

* Logical network isolation.
* Custom IP addressing.
* Ability to define routing and security at the network level.

A screenshot of a computer

AI-generated content may be incorrect.

## Phase 3: Subnet Creation

Created six subnets distributed across two Availability Zones:

* **Public Subnets (Web Tier)**: Host public-facing ALB and Web EC2 instances.
* **Private Subnets (App Tier)**: Host internal ALB and App EC2 instances.
* **Private Subnets (DB Tier)**: Host RDS MySQL instance.  
  Each tier is isolated to enhance security and fault tolerance.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

Phase 4: Internet Gateway and NAT Gateway

* **Internet Gateway (IGW)**: Allows resources in public subnets to access the internet.
* **NAT Gateway**: Enables private subnet instances (App/DB tiers) to access the internet for updates without being directly exposed.

A screenshot of a computer

AI-generated content may be incorrect.

## Phase 5: Route Table Creation

**Public Route Table**: Routes outbound internet traffic from public subnets via IGW.

**Private Route Tables**: Routes outbound traffic from private subnets through NAT Gateway.  
This ensures correct routing for each tier.

A screenshot of a computer

AI-generated content may be incorrect.

## Phase 6: Route Table Association

Linked subnets to their respective route tables:

* Public subnets → Public Route Table.
* Private subnets (App/DB) → Private Route Tables.  
  This enforces intended traffic flow and isolation.

A screenshot of a computer

AI-generated content may be incorrect.

## Phase 7: Security Groups

Created tier-specific Security Groups:

* **Web Tier SG**: Allows inbound HTTP/HTTPS from 0.0.0.0/0.
* **App Tier SG**: Allows inbound HTTP from Web Tier SG only.
* **DB Tier SG**: Allows inbound MySQL (3306) from App Tier SG only.
* **ALB SGs**: Allow traffic from intended sources (public for Web ALB, Web SG for App ALB).  
  Applied **principle of least privilege**A screenshot of a computer program

  AI-generated content may be incorrect.A screenshot of a computer program

  AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Phase 8: IAM

Provisioned IAM roles and instance profiles:

* **EC2 Role**: Grants access to S3 and SSM Parameter Store.
* **Policies**: Attached managed and custom policies for required permissions.  
  Attached IAM instance profile to EC2 instances to enable secure, credential-free AWS service access.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

## Phase 9: Key Pair Creation and Storing

Generated AWS Key Pair for SSH access:

* Stored .pem file securely.
* Associated with EC2 instances for secure administrative access.

A screenshot of a computer

AI-generated content may be incorrect.

## Phase 10: RDS Creation

Deployed **Amazon RDS MySQL** instance:

* Multi-AZ deployment in private DB subnets.
* Security Group restricts access to App Tier only.

A screenshot of a computer program

AI-generated content may be incorrect.

## Phase 11: Test Instance Creation

Launched temporary EC2 instances in Web and App tiers:

* Verified routing, internet access, and inter-tier communication.
* Tested DB connectivity from App tier to RDS MySQL.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

## Phase 11: Application Load Balancer, Target Groups, Auto Scaling Group

## App Tier

* **Internal ALB**: Routes traffic from Web Tier to App Tier.
* **Target Group**: Health checks on App EC2 instances.
* **Launch Template**: User data to configure App EC2 (PHP, DB connection).
* **ASG**: Ensures availability and scales based on demand.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

## Web Tier

* **Public ALB**: Routes public HTTP/HTTPS requests.
* **Target Group**: Health checks on Web EC2 instances.
* **Launch Template**: User data to deploy static files from S3 and proxy /api calls to App ALB.
* **ASG**: Maintains desired capacity and handles scaling events.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Phase 12: S3\_SSM Implementation

* **S3 Bucket**: Stores static assets and application code.
* **SSM Parameter Store**: Stores DB credentials and endpoint securely.
* EC2 instances retrieve configuration from Parameter Store at runtime.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

## Phase 14: Outputs

Defined Terraform outputs:

* Public ALB DNS.
* Internal ALB DNS.
* RDS MySQL endpoint.
* DB name.

A screenshot of a computer

AI-generated content may be incorrect.

## User Interface

### HomePage

A screenshot of a computer

AI-generated content may be incorrect.

### Add Employee

A screenshot of a computer

AI-generated content may be incorrect.

### Data Input (form)

A screenshot of a computer

AI-generated content may be incorrect.

### Form Submission

A screenshot of a computer

AI-generated content may be incorrect.

### View Employees (Data Fetch from RDS)

A screenshot of a computer

AI-generated content may be incorrect.