

# AWS Three-Tier Architecture Web Deployment

## 1. Project Overview

This document outlines the design, implementation, and estimated costs for a secure, scalable, and highly available three-tier architecture on AWS. This architecture, following AWS best practices, is suitable for applications with varying traffic loads and critical data requirements. The architecture incorporates multiple AWS services like VPC, EC2, RDS, S3, and more to provide robust performance, security, and fault tolerance.

## Solution Architecture

### 2. Architecture Layers

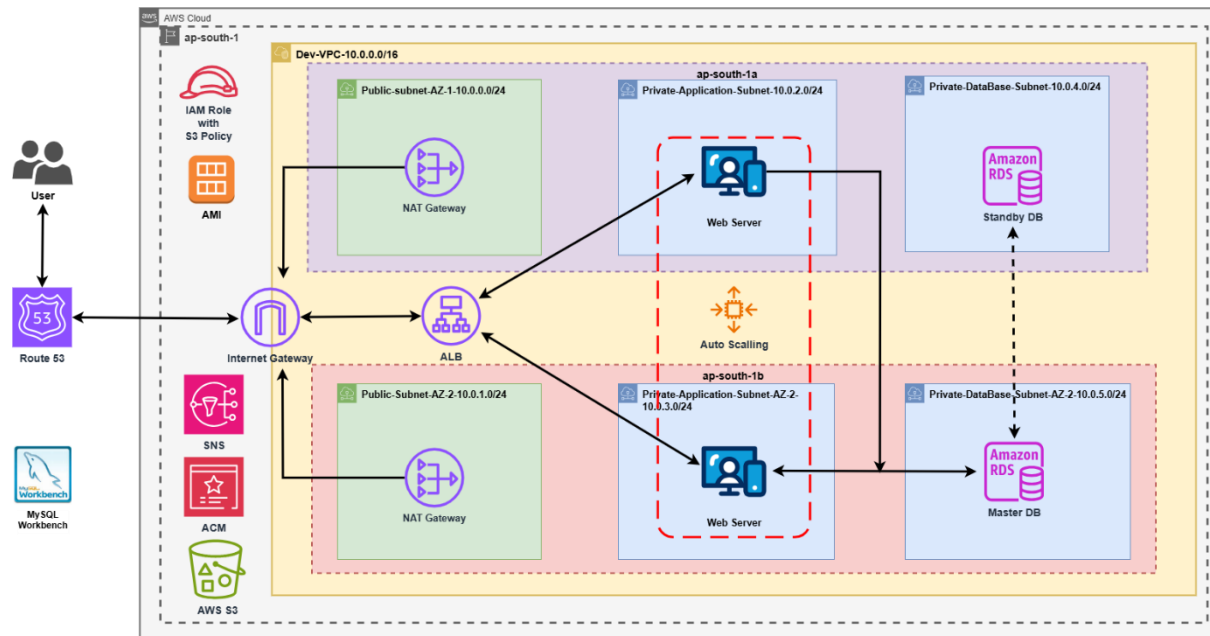
- Presentation Layer (Public Subnet):** Hosts the Application Load Balancer (ALB) and NAT Gateways.
- Application Layer (Private App Subnet):** Contains EC2 instances for the application servers, managed by an Auto Scaling group.
- Data Layer (Private Data Subnet):** Hosts a MySQL RDS instance in Multi-AZ mode for data storage and redundancy.

#### 2.1 Key AWS Services

Service	Purpose
Amazon VPC	Isolates the application resources within a private network.
Subnets	Separates public and private resources for security.
Internet Gateway	Allows public subnet resources to access the internet.
NAT Gateway	Enables internet access for private subnet resources.
EC2 Instances	Hosts the application servers.
Auto Scaling Group	Adjusts the number of EC2 instances based on traffic.
Application Load Balancer	Distributes traffic across EC2 instances.
Amazon RDS (MySQL)	Provides a managed database solution with high availability.
Amazon S3	Stores application assets and backups.
Route 53	Manages DNS for high availability and failover.
IAM Roles	Manages permissions and access for resources.
Certificate Manager	Provides SSL/TLS certificates for encrypted connections.

Below is an architecture diagram that illustrates the three-tier setup and the components involved.

**Figure 1: AWS Three-Tier Architecture Design**



The diagram depicts a VPC with public and private subnets across multiple availability zones, along with key AWS components like ALB, EC2 instances, NAT gateways, and RDS in a Multi-AZ configuration.

## **Solution Components and Configuration**

### **3.1 Networking**

- **VPC:** A dedicated Virtual Private Cloud (CIDR: 10.0.0.0/16) provides network isolation.
- **Subnets:** Two public subnets for ALB and NAT Gateways, and two private subnets for EC2 instances and the RDS database, distributed across two availability zones (AZs) for redundancy.
- **Internet Gateway and NAT Gateways:** The Internet Gateway allows public resources to access the internet, while the NAT Gateways in each public subnet enable private subnet resources to initiate outbound internet connections for updates.

### **3.2 Application Hosting**

- **EC2 Instances:** The application servers are hosted on Amazon EC2 instances within private subnets. Instances are deployed in multiple AZs to ensure high availability.

- **Auto Scaling Group:** Automatically scales the number of EC2 instances based on traffic to handle varying loads. This reduces costs during off-peak hours by scaling down and maintains performance during peak times.
- **Application Load Balancer (ALB):** Manages incoming traffic and distributes it across the EC2 instances. ALB enhances the user experience by ensuring balanced traffic distribution and enables SSL termination for secure connections.

### 3.3 Database Layer

- **Amazon RDS (MySQL):** The MySQL RDS database is set up in a Multi-AZ configuration to ensure high availability. In case of a failure in the primary database, AWS automatically promotes the standby database to ensure uninterrupted access.
- **Backups and Snapshots:** Automated backups and point-in-time recovery capabilities are configured for data protection.

### 3.4 Storage and Static Content

- **Amazon S3:** Used for storing static files and application assets, providing cost-effective, durable storage. S3 integrates with CloudFront (if required) for content delivery.

### 3.5 Security

- **IAM Roles and Policies:** Access to services and resources is controlled using IAM roles and policies, ensuring least-privilege access for all components.
- **Security Groups:** Security groups are configured to restrict traffic at each layer, ensuring only necessary communication is allowed.
- **AWS Certificate Manager:** SSL/TLS certificates encrypt data in transit, protecting sensitive information between the client and application servers.
- **VPC Flow Logs:** Logs are enabled to monitor IP traffic within the VPC, adding an extra layer of security visibility.

### 3.6 Domain and DNS Management

- **Route 53:** Amazon Route 53 manages the application's DNS settings, enabling reliable and low-latency routing for users globally. Route 53 also supports failover to ensure continued service availability in the event of issues.

### 3.7 Monitoring and Notifications

- **Amazon CloudWatch:** Monitors the performance of EC2 instances, RDS, and other AWS resources, providing metrics and setting alarms for resource health.
- **SNS (Simple Notification Service):** Configured to send alerts for critical events, such as scaling events, high CPU usage, or database failover.

---

## Estimated Costs

### 4.1 EC2 and Auto Scaling

- **EC2 Instances:** Approx. \$0.02 per hour for t3.medium instances in a multi-AZ setup.
- **Auto Scaling Group:** No additional charge; charges are only for the EC2 instances it scales.

**Monthly Estimate (approx.): \$30 - \$100 (varies with load).**

### 4.2 Database

- **Amazon RDS (MySQL):** Multi-AZ db.t3.micro instance, approx. \$15 - \$40 per month.

**Backup Storage:** Charged based on usage (first 20 GB free per month).

### 4.3 Storage

- **Amazon S3:** Approx. \$0.023 per GB per month (standard storage) and \$0.004 per 1,000 requests.

**Monthly Estimate: \$1 - \$10 (depending on storage needs).**

### 4.4 Load Balancer

- **Application Load Balancer:** Approx. \$0.0225 per ALB-hour plus \$0.008 per LCU-hour.

**Monthly Estimate: \$15 - \$30.**

### 4.5 Network and Data Transfer

- **NAT Gateway:** Approx. \$0.045 per hour and \$0.045 per GB of data processed.

**Monthly Estimate: \$20 - \$50 (varies with usage).**

### 4.6 DNS and Domain

- **Route 53:** \$0.50 per hosted zone per month, plus \$0.40 per million queries.

**Monthly Estimate: \$1 - \$2.**

### 4.7 Monitoring and Notifications

- **CloudWatch:** Basic monitoring free; charges apply for additional metrics and alarms.

- **SNS:** \$0.50 per million publish requests.

**Monthly Estimate: \$1 - \$5.**

AWS Component	Description	Unit Cost	Monthly Estimate
<b>EC2 Instances</b>	Application servers in multiple AZs	\$0.02 per hour (t3.medium)	\$30 - \$100
<b>Auto Scaling</b>	Scales EC2 instances based on traffic	No additional charge	Based on EC2 usage
<b>Application Load Balancer</b>	Distributes traffic to EC2 instances	\$0.0225 per ALB-hour + \$0.008 per LCU-hour	\$15 - \$30
<b>Amazon RDS (MySQL)</b>	Multi-AZ MySQL database	\$0.017 per hour (db.t3.micro)	\$15 - \$40
<b>Database Backup Storage</b>	Storage for RDS backups	\$0.095 per GB after first 20 GB free	Based on usage
<b>NAT Gateway</b>	Provides internet access for private subnets	\$0.045 per hour + \$0.045 per GB	\$20 - \$50
<b>Amazon S3</b>	Stores static files and application assets	\$0.023 per GB	\$1 - \$10
<b>Route 53</b>	DNS management and routing	\$0.50 per hosted zone + \$0.40 per million queries	\$1 - \$2
<b>AWS Certificate Manager</b>	SSL/TLS certificates for secure connections	Free (for public certificates)	Free
<b>CloudWatch Monitoring</b>	Monitors resource health and sets alarms	Free (basic), additional for custom metrics	\$1 - \$5
<b>SNS (Simple Notification Service)</b>	Sends notifications for alerts and scaling events	\$0.50 per million publish requests	\$1 - \$5

| **Total Estimated Monthly Cost** | **\$100 - \$250**, depending on usage and traffic |

## Benefits

1. **High Availability and Fault Tolerance:** Multi-AZ deployment ensures that the application remains operational even if one AZ fails.
2. **Scalability:** Auto Scaling adjusts the number of application servers based on demand, minimizing costs during low traffic and scaling during peak times.
3. **Security:** IAM policies, VPC isolation, security groups, and encrypted connections provide a secure environment for data and resources.
4. **Performance:** The load balancer ensures even traffic distribution, reducing server load and improving response times.

5. **Cost-Effective:** The use of S3 for storage, auto-scaling, and reserved instances where possible, keeps operational costs optimized.
- 

## Implementation Steps

1. **Create VPC, Subnets, and Networking:** Set up the VPC with public and private subnets, Internet Gateway, and NAT Gateway.
  2. **Deploy EC2 Instances and Auto Scaling Group:** Launch the application servers with an auto-scaling configuration.
  3. **Configure Application Load Balancer:** Set up the ALB to distribute traffic to the EC2 instances.
  4. **Provision Amazon RDS (MySQL):** Set up a MySQL database in Multi-AZ mode with automated backups.
  5. **Set Up Storage with S3:** Store static files and backups in S3 with IAM policies for secure access.
  6. **Implement DNS with Route 53:** Configure DNS settings for domain routing.
  7. **Configure Monitoring and Alarms:** Set up CloudWatch and SNS for monitoring and notifications.
  8. **Security Configurations:** Apply IAM roles, security groups, and SSL certificates.
- 

## Conclusion

This AWS architecture provides a secure, scalable, and high-performance environment for hosting web applications. The design focuses on ensuring high availability, data security, and cost-efficiency. With the modular and scalable nature of AWS services, this solution is flexible and can grow alongside your business needs.