XYZ Platform – AWS Architecture Overview

A scalable , secure, and highly available cloud architecture designed

1. Architecture Summary

- **Deployment Model**: Multi-AZ (Availability Zone) for fault tolerance.
- **Tiered Design**:
    - **Web Tier**: User-facing layer (frontend).
    - **App Tier**: Business logic & microservices.
    - **Data Tier**: Databases & storage.
- **Scalability**: Auto-scaling, serverless components, and managed services.

2. Core Components

2.1 Networking & Subnets

- **VPC (Virtual Private Cloud)**: Isolated network environment.
    - **Public Subnets (2+)**:
        - NAT Gateways (for private instance internet access).
        - Load Balancers.
    - **Private Subnets (3+ per AZ)**:
        - **Web Tier**: Frontend servers (e.g., EC2, ECS).
        - **App Tier**: Backend services (e.g., EC2, Lambda, EKS).
        - **Data Tier**: Databases (e.g., RDS, DynamoDB).

2.2 Traffic Routing & Load Balancing

- **DNS & Routing**:
    - **Amazon Route 53**: Domain management & latency-based routing.
- **Security & Traffic Filtering**:
    - **AWS WAF**: Protects against SQLi, XSS, DDoS.
    - **AWS Shield**: DDoS protection for ALB/CloudFront.
- **Content Delivery**:

  - **CloudFront**: CDN for static/media content.
  - **ALB (Application Load Balancer)**: Distributes traffic to web/app tiers.

2.3 Compute Layer

- **Web Tier**:
  - EC2 Auto Scaling Groups (ASG) or Containers (ECS/EKS).
- **App Tier**:
  - Microservices (Lambda, ECS Fargate).
  - Event-driven processing (SQS, EventBridge).
- **Serverless Options**:
  - API Gateway + Lambda for APIs.

2.4 Data Layer

- **Primary Database**:
  - **Amazon RDS (Multi-AZ)**: For relational data (PostgreSQL/MySQL).
  - **DynamoDB**: NoSQL for high-speed queries.
- **Caching**:
  - **ElastiCache (Redis/Memcached)**: Session/store caching.
- **File Storage**:
  - **Amazon S3**: Static assets, user uploads.
  - **EFS**: Shared file storage for EC2.

2.5 Security

- **Identity & Access**:
  - **IAM**: Least-privilege roles for EC2/Lambda.
  - **Cognito**: User authentication.
- **Network Security**:
  - **Security Groups (SGs)**: Tier-specific traffic rules.
  - **NACLs (Network ACLs)**: Subnet-level firewall.

- **Encryption**:
    - KMS for data-at-rest, TLS for in-transit.

2.6 Monitoring & Operations

- **Observability**:
    - **CloudWatch**: Logs, metrics, alarms.
    - **X-Ray**: Distributed tracing.
- **Alerts**:
    - **SNS**: Notifications for failures/thresholds.
- **CI/CD**:
    - **CodePipeline/CodeDeploy**: Automated deployments.

3. High Availability (HA) & Disaster Recovery (DR)

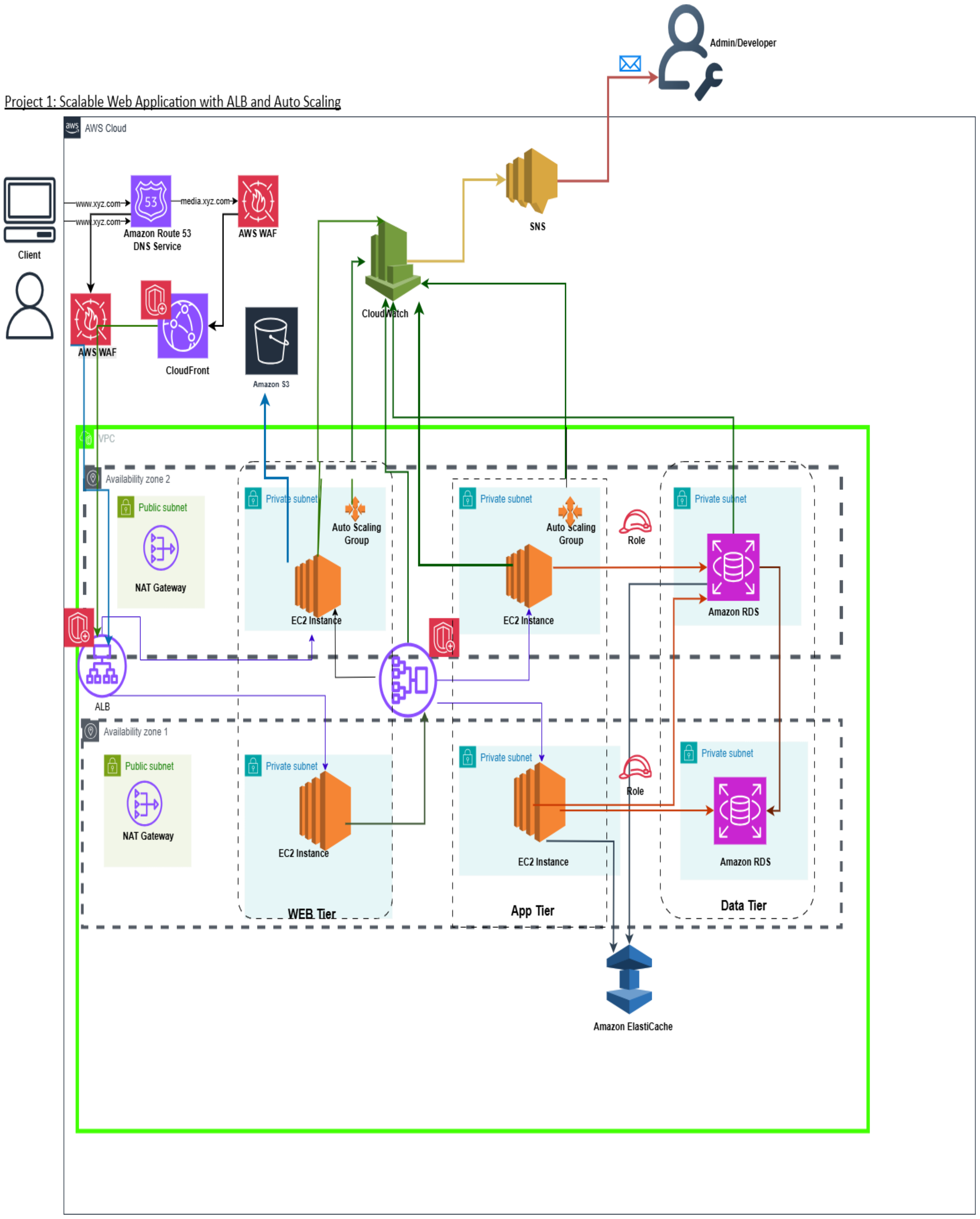
- **Multi-AZ Deployments**: RDS, EC2 ASG.
- **Backups**:
    - RDS snapshots, S3 versioning.
- **Cross-Region Replication**:
    - S3 CRR, DynamoDB Global Tables.

4. Cost Optimization

- **Reserved Instances**: For steady-state workloads.
- **Spot Instances**: For fault-tolerant tasks.
- **Auto Scaling**: Scale down during off-peak.

5. Diagram

Project 1: Scalable Web Application with ALB and Auto Scaling


Admin/Developer
AWS Cloud
SNS
Client
www.xyz.com
www.xyz.com
Amazon Route 53
DNS Service
media.xyz.com
AWS WAF
CloudWatch
AWS WAF
CloudFront
Amazon S3
VPC
Availability zone 2
Public subnet
NAT Gateway
Private subnet
Auto Scaling
Group
EC2 Instance
Private subnet
Auto Scaling
Group
EC2 Instance
Role
Private subnet
Amazon RDS
ALB
Availability zone 1
Public subnet
NAT Gateway
Private subnet
EC2 Instance
WEB Tier
Private subnet
Role
EC2 Instance
App Tier
Private subnet
Amazon RDS
Data Tier
Amazon ElastiCache