BHADRINATH P S **29-JAN-2024** **INSURANCE**

AWS - CASE STUDY QUESTIONS

Scenario: Hosting a Web Application on AWS for IT Professionals

Your organization plans to host a web application on AWS. The application includes:

1. A frontend built using React.
2. A backend API built with Python (Flask/Django).
3. A MySQL database for storing data.

The architecture should:

1. Use highly available and scalable AWS services.
2. Secure the application with best practices.
3. Ensure minimal downtime.

SOLUTION

Frontend (React) Hosting:

- **Amazon S3**: Host the React application as a static website.
- **Amazon CloudFront**: Use for fast content delivery worldwide.
- **Amazon Route 53**: Manage DNS and route traffic to CloudFront.

Backend API (Python with Flask/Django):

- **Amazon EC2**: Host the backend API (Flask/Django) on scalable EC2 instances.
- **Elastic Load Balancer (ALB)**: Distribute traffic across multiple EC2 instances for load balancing.
- **Auto Scaling**: Automatically add/remove EC2 instances based on traffic.

Database (MySQL):

- **Amazon RDS**: Use RDS for a fully managed MySQL database with automated backups.
- **Multi-AZ Deployment**: Enable high availability for the database by replicating data across multiple availability zones.

Security:

- **IAM (Identity and Access Management)**: Use for secure access control to AWS resources.
- **Security Groups**: Control network traffic between your EC2 instances and RDS.
- **AWS WAF**: Protect the application from common web threats like SQL injection and cross-site scripting.

High Availability & Scaling:

- **Auto Scaling**: Automatically scale EC2 instances based on demand.
- **RDS Multi-AZ**: Ensure high availability of the MySQL database.
- **Elastic Load Balancer (ALB)**: Distribute incoming traffic to available EC2 instances.

Minimal Downtime:

- **Rolling Deployments**: Deploy updates to EC2 instances without downtime using services like **Elastic Beanstalk** or **CodeDeploy**.
- **Backup & Recovery**: Use automated RDS backups and S3 for storing critical data.