Name:AbdelRahman Moustafa Mohamed Abdallah

Groub name: AWS Cloud Specialist (ALX1_SWD8_M1e)

Student ID: 1110242719

Email: abdulrahmanmoustafa2002@gmail.com

**Project 1: Building a Highly Available, Scalable Web Application**

**Project 2: Securing and Monitoring Resources with AWS**

Supervise by: Eng. Merhan Adel

# Badges Link

# Week 1: Project 1 : AWS Project: Building a Highly Available, Scalable Web Application

**Objective:**
To design and deploy a highly available, scalable, and secure web application using AWS services. The architecture will follow the AWS Well-Architected Framework principles and ensure the application meets the needs of Example University during peak admissions periods.

---

**Tasks and Deliverables**

1. **Planning and Design:**
    - **Review the principles of the AWS Well-Architected Framework, focusing on Security, Reliability, Performance Efficiency, Cost Optimization, and Operational Excellence.**
    - **Create an architectural diagram that demonstrates how AWS services such as EC2 (for web servers), RDS (for database), and VPC (for networking) will interact.**
    - **Estimate the cost of running the solution for 12 months using the AWS Pricing Calculator.**

**Deliverables:**

- **Architectural diagram illustrating AWS service interactions (EC2, RDS, VPC, ELB).**
- **Initial cost estimate using the AWS Pricing Calculator.**

2. **Deploying the Basic Web Application:**
    - **Deploy a functional web application on a single EC2 instance running Ubuntu, with a MySQL database hosted on Amazon RDS.**
    - **Set up a Virtual Private Cloud (VPC) with both public and private subnets, ensuring security while allowing the application to be publicly accessible.**
    - **Ensure the separation of the web server and database layers to maintain a modular and scalable architecture.**

**Deliverables:**

- **Deployed web application on an EC2 instance with a MySQL database in RDS.**
- **A VPC configured for public accessibility and security.**

3. **Implementing Load Balancing and Security Configuration:**
    - **Set up an Elastic Load Balancer (ELB) to distribute incoming traffic across multiple EC2 instances, ensuring high availability.**

- **Configure security groups, IAM roles, and Network ACLs to secure the web servers and RDS database.**
- **Verify that the VPC and subnets are properly configured to support secure networking and performance optimization.**

**Deliverables:**

- **Load-balanced web application deployed across multiple EC2 instances.**
- **Correct network security configurations for EC2 and RDS (e.g., security groups, IAM roles).**

4. **Decoupling the Application Components:**
   - **Migrate the database from the EC2 instance to a dedicated Amazon RDS instance.**
   - **Use AWS Secrets Manager to securely store and manage database credentials, ensuring the web application accesses the database securely.**
   - **Reconfigure the web application to connect securely to the Amazon RDS instance.**

**Deliverables:**

- **Web application connected to the RDS database via AWS Secrets Manager.**
- **Documentation of the migration process and updated configurations.**

5. **Implementing Auto Scaling and Testing:**
   - **Configure Auto Scaling to dynamically manage the number of EC2 instances based on traffic and application load.**
   - **Run load tests to simulate high traffic and monitor how the application scales under increased demand.**
   - **Conduct security and performance tests to ensure that the infrastructure is secure and meets high availability requirements.**

**Deliverables:**

- **Auto Scaling configuration with scaling policies in place.**
- **Load test results demonstrating scalability and performance under load.**

6. **Cost Optimization and Final Review:**
   - **Revisit the AWS Pricing Calculator to finalize the cost estimate based on the fully deployed architecture.**
   - **Review the deployed solution to identify potential areas for cost optimization without compromising performance or security.**

**Deliverables:**

- **Finalized cost estimate using the AWS Pricing Calculator.**
- **Cost optimization recommendations for the solution.**

7. **Final Report and Presentation:**
    - **Compile a comprehensive report that summarizes the architecture, configurations, test results, and final cost estimation.**
    - **Prepare a presentation of the project, highlighting key architecture components, scalability, and security features, as well as the cost benefits of the deployed solution.**

**Deliverables:**

- **Final project report detailing the architecture, security, performance, scalability, and cost estimates.**
- **Presentation slides summarizing the project for stakeholders.**

# Week 2 Project 2: AWS Project: Securing Data, Network, and Resources

**Objective:**
To implement security measures across Amazon S3, VPCs, and AWS resources in compliance with AnyCompany Financial's regulatory and security requirements. The architecture will ensure data protection, secure networking, and continuous monitoring of AWS resources to safeguard against unauthorized access and breaches.

---

**Tasks and Deliverables**

1. **Phase 1: Securing Data in Amazon S3**

**Tasks:**

- Limit access to Amazon S3 buckets to specific account managers by using IAM policies and assigning them to the Account Manager group.
- Enable versioning for all S3 buckets to track and preserve multiple versions of objects.
- Enable object logging for all S3 buckets to monitor access and changes to the data.
- Encrypt all buckets with server-side encryption using Amazon S3-managed keys (SSE-S3) to ensure data at rest is protected.
- Set up Amazon S3 Inventory to maintain a running inventory of all objects stored in the S3 buckets for auditing and monitoring purposes.
- Conduct a cost assessment to secure Amazon S3 storage with the implemented security features.

**Deliverables:**

- Access controls for Amazon S3 buckets restricted to account managers.
- Versioning and logging enabled for S3 buckets.
- Server-side encryption (SSE-S3) implemented on all S3 buckets.
- Amazon S3 Inventory configured for file tracking.
- Cost assessment report for securing Amazon S3.

---

2. **Phase 2: Securing VPCs**

**Tasks:**

- Analyze the existing LabVPC and WebServer instance configurations, correct network misconfigurations, and implement best practices for securing VPCs.
- Update security groups to limit access to the web servers, ensuring only approved IP addresses can access the web servers over necessary ports.

- Implement proper routing tables and subnets for secure traffic flow between the public and private parts of the VPC.
- Configure network ACLs (Access Control Lists) to add another layer of security for inbound and outbound traffic.
- Ensure VPC peering and NAT gateways are correctly configured for secure and efficient traffic routing.

**Deliverables:**

- Corrected and secured VPC configuration.
- Updated security groups with restricted access to the web servers.
- Proper routing tables, subnets, and network ACLs configured for secure traffic flow.
- Documentation of VPC security enhancements and corrections.

---

3. **Phase 3: Securing AWS Resources Using AWS KMS**

**Tasks:**

- Implement a mechanism to create and manage AWS KMS customer-managed keys for encryption purposes.
- Use AWS KMS to encrypt data stored in Amazon S3 and the root volume of the EC2 instance (EBS encryption).
- Configure AWS Secrets Manager to store sensitive information (such as database credentials) and encrypt the secrets using the customer-managed KMS keys.
- Ensure that all sensitive data, including PII, credit card numbers, and social security numbers, are encrypted in line with regulatory compliance standards.

**Deliverables:**

- AWS KMS customer-managed keys created and managed for encryption.
- Data in Amazon S3 and EC2 EBS volumes encrypted using AWS KMS.
- Secrets stored in AWS Secrets Manager encrypted with customer-managed keys.
- Documentation of encryption policies and compliance with regulations.

---

4. **Phase 4: Monitoring and Logging**

**Tasks:**

- Set up AWS CloudTrail to track all API calls to Amazon S3, ensuring that any access or modifications to data are logged and traceable.

- Configure CloudWatch Logs to monitor the WebServer instance's authentication logs, allowing real-time monitoring of access attempts and security breaches.
- Create a CloudWatch alarm to notify team members when there are unauthorized access attempts or suspicious activities on the WebServer instance.
- Use AWS Config to monitor AWS resource configurations and ensure that S3 buckets are always created with object logging enabled. Automatically remediate any misconfigurations.
- Implement notifications via SNS or other channels to alert the team in case of any security incidents.

**Deliverables:**

- CloudTrail enabled for logging all API calls to Amazon S3.
- CloudWatch Logs configured to monitor WebServer authentication.
- CloudWatch alarm created to notify of security incidents.
- AWS Config configured to enforce security compliance (S3 logging enabled).
- Documentation of monitoring, logging, and alerting systems.