رواد مصر الرقمية

وزارة الاتصـــالات
وتكنولوجيا المعلومات

Name: Yousef Hassan Yousef Eltobgy

Student ID: 21031713

Email: eltobgyy@gmail.com

Track: AWS Cloud Solution Admin & Architect

Group Code: ALX1_ISS4_M1e

Project Instructions for Students:-

The graduation project is a key requirement for obtaining the Digital Egypt Pioneers Initiative Completion Certificate.

- Students are free to choose any of the ideas listed in the project booklet for their respective career track without any restrictions, they are able to choose other ideas not listed in the booklet but it should go in the same format of the ideas given.
- The project is a group assignment, and teams should consist of 4 to 6 students.
- Within a maximum of one week from the announcement of the project booklet, students must form their groups and inform the instructor. If they fail to do so, the instructor has the right to assign groups randomly and announce the team members.
- Students must divide the work responsibilities within the group and inform the instructor within two weeks of the project booklet announcement. During the final presentation, each group must demonstrate the work completed and each member's responsibility for their assigned tasks.
- The final evaluation will be based on the final presentation, which must include the students' adherence to the deliverables and the distribution of tasks among team members.

تعليمات المشروع للطلاب:- مشروع التخرج هو أحد المتطلبات الأساسية للحصول على شهادة إتمام

مبادرة رواد مصر الرقمية.

- يتمتع الطلاب بحرية اختيار أي من الأفكار المدرجة في كتيب المشروع لمسارهم الوظيفي دون أي قيود، أو اختيار أي فكره أخرى غير مدرجه بالكتيب ولكن بنفس المنهاج المستخدم في الأفكار المعطى .
- المشروع عمل جماعي، ويجب أن تتكون فرق العمل من 4 إلى 6 طلاب.
- في غضون أسبوع كحد أقصى من إعلان كتيب المشروع، يجب على الطلاب تشكيل فرقهم وإبلاغ المدرب بذلك. في حالة عدم القيام بذلك، يحق للمدرب تقسيمهم بشكل عشوائي وإعلان أعضاء الفريق.
- يجب على الطلاب تقسيم مسؤوليات العمل داخل المجموعة وإبلاغ المدرب بها في غضون أسبوعين من إعلان كتيب المشروع. كما يجب على كل مجموعة خلال العرض النهائي توضيح الأعمال التي تم إنجازها وتحديد مسؤولية كل فرد في تنفيذها.
- سيتم التقييم النهائي بناءً على العرض النهائي، والذي يجب أن يتضمن التزام الطلاب بتسليم المخرجات وتقسيم العمل بين أعضاء الفريق.

Project 1. Building a Highly Available, Scalable Web Application

Week 1: Planning the design and estimating cost

- **Task**: Planning the design and estimating cost
  - Creating an architectural diagram
  - Developing a cost estimate
- **Deliverables**: Create an architectural diagram to illustrate what you plan to build. Consider how you will accomplish each requirement in the solution, and Develop a cost estimate that shows the cost to run the solution in the us-east-1 Region for 12 months.

Week 2: Creating a basic functional web application.

- **Task**: Creating a basic functional web application
  - Creating a virtual network
  - Creating a virtual machine
  - Testing the deployment
- **Deliverables**: Create a virtual network to host the web application, Create a virtual machine in the cloud to host the web application, and Test the deployment of the web application to ensure it is accessible from the internet and functional. Perform a few tasks, such as viewing, adding, deleting, or modifying records.

Week 3: Decoupling the application components, and

- **Task 1**: Decoupling the application components
  - Changing the VPC configuration
  - Creating and configuring the Amazon RDS database
  - Configuring the development environment
  - Provisioning Secrets Manager
  - Provisioning a new instance for the web server
  - Migrating the database
  - Testing the application
- **Deliverables**:
  - Update or re-create the virtual network components that are necessary to support hosting the database separately from the application.
  - Create an Amazon Relational Database Service (Amazon RDS) database that runs a MySQL engine. You can choose to create a provisioned instance or run it serverlessly
  - Provision an AWS Cloud9 environment to run AWS Command Line Interface (AWS CLI) commands in later tasks.
  - Use AWS Secrets Manager to create a secret to store the database credentials, and configure the web application to use Secrets Manager.
  - Create a new virtual machine to host the web application.
  - Migrate the data from the original database, which is on an EC2 instance, to the new Amazon RDS database.
  - Access the application and perform a few tasks to test it. For example, view, add, delete, and modify student records.

Week 4: Implementing high availability and scalability

- **Task**: Implementing high availability and scalability
    - Creating an Application Load Balancer
    - Implementing Amazon EC2 Auto Scaling
    - Accessing the application
    - Load testing the application
- **Deliverables**: Launch a load balancer, Create a new launch template, and use an Auto Scaling group to launch the EC2 instances that host the web application, Access the application and perform a few tasks to test it. For example, view, add, delete, and modify student records, and Perform a load test on the application to monitor scaling.

Project 2. Securing and Monitoring Resources with AWS

Week 1: Securing data in Amazon S3

- **Task**: Securing data in Amazon S3
  - Create a bucket, apply a bucket policy, and test access
  - Enable versioning and object-level logging on a bucket
  - Implement the S3 Inventory feature on a bucket
  - Confirm that versioning works as intended
  - Confirm object-level logging and query the access logs by using Athena
  - Review the S3 Inventory report by using S3 Select Cost assessment to secure Amazon S3
- **Deliverables**: create a bucket, apply a bucket policy to it, enable versioning and object-level logging on the data-bucket, enable the S3 Inventory feature to monitor changes to objects that are stored in an S3 bucket, access the AWS account as the paulo user and upload an object to the data-bucket, confirm the S3 object-level logging you enabled earlier is successfully writing log data to S3, and does your use of these Amazon S3 security features result in additional cost in the account? If so, how much do you estimate that it will cost?

Week 2: Securing VPCs

- **Task**: Securing VPCs
  - Review LabVPC and its associated resources
  - Create a VPC flow log
  - Access the WebServer instance from the internet and review VPC flow logs in CloudWatch
  - Configure route table and security group settings
  - Secure the WebServerSubnet with a network ACL
  - Review NetworkFirewallVPC and its associated resources
  - Create a network firewall
  - Create route tables
  - Configure logging for the network firewall
  - Configure the firewall policy and test access Cost estimate to secure a VPC with a network firewall
- **Deliverables**: familiarize yourself with resources that already exist in the lab environment, create a VPC flow log for LabVPC, use your web browser to test access to the WebServer EC2 instance over port 80 (HTTP), create a route for traffic from the internet to access the WebServerSubnet through an internet gateway, configure a network access control list (ACL) to secure the subnet where the web server is running, work to secure a different VPC, named NetworkFirewallVPC, create a network firewall for the NetworkFirewallVPC, create and configure three new route tables, including one for each subnet in the NetworkFirewallVPC and one to handle inbound (ingress) traffic for the internet gateway in NetworkFirewallVPC, configure logging for the network firewall so that you can analyze details of network traffic requests, and define and add a stateful rule group to the network firewall's policy. And Use the AWS Pricing Calculator and the information from the previous table to create a detailed pricing estimate for the network firewall.

Week 3: Securing AWS resources by using AWS KMS

- **Task**: Securing AWS resources by using AWS KMS
  - Create a customer managed key and configure key rotation
  - Update the AWS KMS key policy and analyze an IAM policy
  - Use AWS KMS to encrypt data in Amazon S3
  - Use AWS KMS to encrypt the root volume of an EC2 instance
  - Use AWS KMS envelope encryption to encrypt data in place
  - Use AWS KMS to encrypt a Secrets Manager secret
  - Cost assessment for using AWS KMS
- **Deliverables**: create an AWS KMS customer managed key. You will then configure automatic key rotation on the key, modify the policy of the AWS KMS key that you created so that the sofia user will be authorized to use the key, use the AWS KMS key that you created to encrypt an object in the data-bucket S3 bucket, use the AWS KMS key again, but now you will use it to encrypt the root volume of a new EC2 instance, use the AWS Command Line Interface (AWS CLI) to encrypt data in place by using the AWS KMS key, create a key-value pair (a secret), which you will encrypt with your AWS KMS key and store in Secrets Manager, and does your use of AWS KMS result in additional cost in the account? If so, what usage would you be charged for?

Week 4: Monitoring and logging

- **Task**: Monitoring and logging
  - Use CloudTrail to record Amazon S3 API calls
  - Use CloudWatch Logs to monitor secure logs
  - Create a CloudWatch alarm to send notifications for security incidents
  - Configure AWS Config to assess security settings and remediate the configuration of AWS resources
  - Cost assessment for monitoring and logging
- **Deliverables**: use CloudTrail to record API calls that are made to Amazon S3 buckets, configure CloudWatch Logs to monitor SSH access to the instance so that your company can understand who accesses the server, where they access it from, when they access it, and what actions they take, create a CloudWatch alarm to notify these team members when such an incident occurs, use AWS Config to report on whether object logging is configured on the S3 buckets in the AnyCompany Financial account, and does your use of CloudTrail, CloudWatch, and AWS Config security features result in additional cost in the account? If so, how much do you estimate that it will cost?