AWS Cloud Specialist

Project 1: Deploying a Scalable Web Application on AWS

Description: This project involves designing and deploying a database-driven web application in the AWS Cloud, leveraging AWS services without step-by-step guidance. The architecture should adhere to the principles of the AWS Well-Architected Framework, ensuring it is highly available, scalable, performant, and secure.

Week 1: Project Planning and Architectural Design

Tasks:

- Review the principles of the AWS Well-Architected Framework (Security, Reliability, Performance Efficiency, Cost Optimization, and Operational Excellence).

- Create an architectural diagram illustrating the required AWS services for the web application and their interactions (e.g., using EC2 for the web server, RDS for the database, and VPC for networking).

- Estimate the costs associated with the AWS services using the AWS Pricing Calculator based on the architectural design.

Deliverables:

- Architectural diagram showcasing the interaction of AWS services (e.g., EC2, RDS, VPC, S3).

- Initial cost estimate derived from the AWS Pricing Calculator.

Web Application and Database Deployment

Tasks:

- Deploy a functional web application on a single EC2 instance, supported by a relational database (RDS).

- Set up a Virtual Private Cloud (VPC) to create a virtual network, ensuring the web application is hosted securely and is publicly accessible.

- Architect the application by separating it into a web server layer and a database layer.

Deliverables:

- Deployed web application operating on an EC2 instance with a relational database (RDS).

- A configured VPC ensuring both security and public access.
- Documentation detailing the separation of application layers (web server and database).

Week 2: Load Balancing, Security Configuration, and Network Setup

Tasks:

- Implement a load-balanced web application by distributing traffic across multiple EC2 instances using Elastic Load Balancing (ELB) for high availability.
- Configure security settings for the web servers and database through security groups, network ACLs, and IAM roles.
- Confirm that the VPC and subnets are set up correctly to support secure networking.

Deliverables:

- Load-balanced web application deployed across several EC2 instances.
- Appropriate network security configurations for web servers and the database (e.g., security groups, IAM roles).
- Documentation outlining the network setup and applied security measures.

High Availability, Scalability, and Final Testing

Tasks:

- Configure Auto Scaling for EC2 instances to ensure high availability.
- Test the web application's scalability by simulating load and observing how the infrastructure adapts.
- Conduct final testing of the overall architecture, covering load balancing, security, availability, and performance.
- Finalize cost estimation using the AWS Pricing Calculator based on the deployed infrastructure.

Deliverables:

- Auto Scaling configuration for web servers to guarantee scalability.
- Final testing report summarizing performance, availability, and security evaluations.
- Updated cost estimation for the deployed solution utilizing the AWS Pricing Calculator.
- Comprehensive project report summarizing the architecture, configurations, and results.

Week 3 and final week

Project 2: Securing and Monitoring Resources with AWS

Description:This project aims to secure AWS resources, focusing on data in Amazon S3, VPCs, and AWS Key Management Service (KMS). It will also implement monitoring and logging solutions to ensure ongoing security and compliance.

Securing Data in Amazon S3

Tasks:

- **Create an S3 bucket, apply a bucket policy, and test access to ensure proper permissions.**
- **Enable versioning and object-level logging on the bucket for data protection and auditing.**
- **Implement the S3 Inventory feature to track the contents of the bucket.**
- **Confirm that versioning works correctly by uploading and retrieving different versions of an object.**
- **Verify object-level logging and use Amazon Athena to query the access logs for insights.**
- **Review the S3 Inventory report using S3 Select for efficient data retrieval and analysis.**

Deliverables:

- **Configured S3 bucket with access policies and logging.**
- **Confirmation reports for versioning and object-level logging functionality.**
- **S3 Inventory report reviewed with S3 Select.**
- **Cost assessment for securing Amazon S3.**

Securing VPCs

Tasks:

- **Review the existing LabVPC and its associated resources to understand the current architecture.**
- **Create a VPC flow log to capture traffic information.**

- Access the WebServer instance from the internet and review the VPC flow logs in CloudWatch for monitoring access.
- Configure route tables and security group settings to enhance network security.
- Secure the WebServerSubnet with a network ACL for additional layer of protection.
- Review the NetworkFirewallVPC and its associated resources for compliance and effectiveness.
- Create a network firewall to filter incoming and outgoing traffic.
- Establish route tables to manage traffic flow appropriately.
- Configure logging for the network firewall to monitor activity.
- Set up the firewall policy and test access to ensure security measures are effective.

Deliverables:

- VPC flow logs and access monitoring reports.
- Configuration documentation for route tables, security groups, and network ACLs.
- Firewall setup and logging reports.
- Cost estimate for securing a VPC with a network firewall.

Securing AWS Resources Using AWS KMS

Tasks:

- Create a customer-managed key in AWS KMS and configure key rotation for security.
- Update the KMS key policy and analyze an IAM policy to ensure proper access controls.
- Use AWS KMS to encrypt data stored in Amazon S3, enhancing data security.
- Encrypt the root volume of an EC2 instance using AWS KMS.
- Implement AWS KMS envelope encryption for data at rest.
- Use AWS KMS to encrypt a secret in AWS Secrets Manager for secure credential management.

Deliverables:

- Customer-managed key configurations and policy updates.
- Encryption reports for S3 data, EC2 root volumes, and Secrets Manager secrets.
- Cost assessment for using AWS KMS.

Monitoring and Logging

Tasks:

- Use AWS CloudTrail to record Amazon S3 API calls for auditing and compliance.
- Utilize CloudWatch Logs to monitor and analyze secure logs for security events.
- Create a CloudWatch alarm to notify stakeholders of potential security incidents.
- Configure AWS Config to assess and remediate security settings of AWS resources.

Deliverables:

- CloudTrail logging configuration and access reports.
- CloudWatch Logs monitoring setup and alarm notifications.
- AWS Config compliance assessment report.
- Cost assessment for monitoring and logging solutions.

This structured approach ensures comprehensive security and monitoring across AWS resources while adhering to best practices and optimizing costs.