Cloudly

Assessment for Lead DevOps Engineer

1. Your team is developing a new microservice that will be deployed to a Kubernetes cluster. The microservice requires access to a MySQL database and also it requires access to an API key that is used to access an external service. How would you manage the MySQL credentials and API key securely?
    a. Store the API key and credentials in a Kubernetes Secret.
    b. Store the API key and credentials in a plaintext file.
    c. Store the API key and credentials in a ConfigMap.
    d. Store the API key and credentials in the Docker image.
2. Your team is responsible for managing a fleet of EC2 instances running a web application. You want to make sure that any configuration changes you make to the instances are tracked and recorded for auditing purposes. Which tool would you use for this?
    a. AWS Config
    b. AWS CloudTrail
    c. AWS CloudWatch
    d. AWS Inspector
3. Your team is responsible for deploying a microservices-based application on AWS. The application consists of 10 services, each of which runs in a separate container. What tool would you use to orchestrate the deployment of the containers across the cluster, please provide a working example or a pseudocode.
    a. AWS CloudFormation
    b. AWS Elastic Beanstalk
    c. AWS ECS
    d. AWS Lambda
4. You are responsible for maintaining a production environment with multiple microservices. A new release of one microservice has caused errors that are causing the application to fail. How would you handle this situation?
    a. Roll back the release to the previous version.
    b. Deploy a new release with a fix for the errors.
    c. Monitor the system and wait for the errors to resolve themselves.
    d. Wait for a ticket from the development team to address the errors.
5. Your organization operates a mission-critical database that stores sensitive customer data. You discover a data corruption issue affecting a subset of records. How would you restore the affected data while minimizing downtime and ensuring data integrity?
6. You are responsible for managing a cloud-based e-commerce platform running on an AWS infrastructure. The application utilizes an Amazon RDS database as its backend. Recently,

customers have reported slow response times when interacting with the product search feature. After analyzing the system, you suspect that the underlying cause is a slow database query. Describe the specific steps you would take, using AWS database monitoring and optimization tools, to identify the problematic query and optimize it for better performance in the Amazon RDS database environment.

7. You are responsible for setting up a CI/CD pipeline for a new application. Which tool would you use to automate the building and testing of the application code?
    a. Jenkins
    b. AWS CodePipeline
    c. AWS CodeBuild
    d. AWS Amplify
    e. Travis CI
8. Your organization operates a business-critical application that requires continuous monitoring. How would you design and configure a monitoring system that collects and analyzes relevant metrics and sends real-time alerts to the operations team for anomalies, performance degradation, or system failures?
9. A compliance audit has identified non-compliant configurations in your cloud environment related to access controls and encryption settings. How would you remediate these issues while ensuring minimal disruption to ongoing operations and maintaining continuous compliance?
10. Your organization plans to migrate an on-premises application to the cloud. The application comprises multiple tiers, including a web server, application server, and database server. How would you design the VPC architecture, subnets, and security groups to ensure secure communication between the tiers while limiting access to only necessary resources?
11. Your company operates a distributed system with hundreds of servers, each generating a significant amount of log data. How would you design and implement a centralized log management solution that allows efficient log collection, storage, analysis, and real-time alerting for critical events?
12. A security incident has occurred, and you need to investigate the breach. How would you leverage log data, including access logs, system logs, and application logs, to trace the attacker's actions, identify compromised resources, and determine the extent of the breach?

Last date of assessment submission: 18 June 2023
Submit to: ishmam@cloudly.io
Instruction: Use any editor of your choice, share the public repo of github in email.