DOP-C01 Q&As

AWS Certified DevOps Engineer - Professional (DOP-C01)

Pass Amazon DOP-C01 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/aws-devops-engineer-professional.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Your CTO thinks your AWS account was hacked. What is the only way to know for certain if there was unauthorized access and what they did, assuming your hackers are very sophisticated AWS engineers and doing everything they can to cover their tracks?

A. Use CloudTrail Log File Integrity Validation.

B. Use AWS Config SNS Subscriptions and process events in real time.

C. Use CloudTrail backed up to AWS S3 and Glacier.

D. Use AWS Config Timeline forensics.

Correct Answer: A

You must use CloudTrail Log File Validation (default or custom implementation), as any other tracking method is subject to forgery in the event of a full account compromise by sophisticated enough hackers. Validated log files are invaluable in security and forensic investigations. For example, a validated log file enables you to assert positively that the log file itself has not changed, or that particular user credentials performed specific API activity. The CloudTrail log file integrity validation process also lets you know if a log file has been deleted or changed, or assert positively that no log files were delivered to your account during a given period of time.

Reference: http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-log-file-validation-intro.html

QUESTION 2

A company hosts its staging website using an Amazon EC2 instance backed with Amazon EBS storage. The company wants to recover quickly with minimal data losses in the event of network connectivity issues or power failures on the EC2 instance.

Which solution will meet these requirements?

A. Add the instance to an EC2 Auto Scaling group with the minimum, maximum, and desired capacity set to 1.

B. Add the instance to an EC2 Auto Scaling group with a lifecycle hook to detach the EBS volume when the EC2 instance shuts down or terminates.

C. Create an Amazon CloudWatch alarm for the StatusCheckFailed_System metric and select the EC2 action to recover the instance.

D. Create an Amazon CloudWatch alarm for the StatusCheckFailed_Instance metric and select the EC2 action to reboot the instance.

Correct Answer: A

Reference: https://docs.aws.amazon.com/autoscaling/ec2/userguide/as-maintain-instance-levels.html

QUESTION 3

You work for a startup that has developed a new photo-sharing application for mobile devices. Over recent months, your

application has increased in popularity; this has resulted in a decrease in the performance of the application clue to the increased load. Your application has a two-tier architecture that is composed of an Auto Scaling PHP application tier and a MySQL RDS instance initially deployed with AWS CloudFormation. Your Auto Scaling group has a min value of 4 and a max value of 8. The desired capacity is now at 8 because of the high CPU utilization of the instances. After some analysis, you are confident that the performance issues stem from a constraint in CPU capacity, although memory utilization remains low. You therefore decide to move from the general-purpose M3 instances to the compute-optimized C3 instances.

How would you deploy this change while minimizing any interruption to your end users?

A. Sign into the AWS Management Console, copy the old launch configuration, and create a new launch configuration that specifies the C3 instances. Update the Auto Scaling group with the new launch configuration. Auto Scaling will then update the instance type of all running instances.

B. Sign into the AWS Management Console, and update the existing launch configuration with the new C3 instance type. Add an UpdatePolicy attribute to your Auto Scaling group that specifies AutoScalingRollingUpdate.

C. Update the launch configuration specified in the AWS CloudFormation template with the new C3 instance type. Run a stack update with the new template. Auto Scaling will then update the instances with the new instance type.

D. Update the launch configuration specified in the AWS CloudFormation template with the new C3 instance type. Also add an UpdatePolicy attribute to your Auto Scaling group that specifies AutoScalingRollingUpdate. Run a stack update with the new template.

Correct Answer: D

QUESTION 4

A company wants to ensure that their EC2 instances are secure. They want to be notified if any new vulnerabilities are discovered on their instances, and they also want an audit trail of all login activities on the instances.

Which solution will meet these requirements?

A. Use AWS Systems Manager to detect vulnerabilities on the EC2 instances. Install the Amazon Kinesis Agent to capture system logs and deliver them to Amazon S3.

B. Use AWS Systems Manager to detect vulnerabilities on the EC2 instances. Install the Systems Manager Agent to capture system logs and view login activity in the CloudTrail console.

C. Configure Amazon CloudWatch to detect vulnerabilities on the EC2 instances. Install the AWS Config daemon to capture system logs and view them in the AWS Config console.

D. Configure Amazon Inspector to detect vulnerabilities on the EC2 instances. Install the Amazon CloudWatch Agent to capture system logs and record them via Amazon CloudWatch Logs.

Correct Answer: B

QUESTION 5

You are building a large, multi-tenant SaaS (software-as-a-service) application with a component that fetches data to process from a customer-specific Amazon S3 bucket in their account. How should you ensure that your application follows security best practices and limits risk when fetching data from customer-owned Amazon S3 buckets?

A. Have users create an IAM user with a policy that grants read-only access to the Amazon S3 bucket required by your application, and store the corresponding access keys in an encrypted database that holds their account data.

B. Have users create a cross-account IAM role with a policy that grants read-only access to the Amazon S3 bucket required by your application to the AWS account ID running your production Sass application.

C. Have users create an Amazon S3 bucket policy that grants read-only access to the Amazon S3 bucket required by your application, and securely store the corresponding access keys in the database holding their account data.

D. Have users create an Amazon S3 bucket policy that grants read-only access to the Amazon S3 bucket required by your application and limits access to the public IP address of the SaaS application.

Correct Answer: B