DOP-C02$^{\text{Q\&As}}$

AWS Certified DevOps Engineer - Professional

Pass Amazon DOP-C02 Exam with 100% Guarantee

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

https://www.passapply.com/dop-c02.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A company has multiple accounts in an organization in AWS Organizations. The company\\'s SecOps team needs to receive an Amazon Simple Notification Service (Amazon SNS) notification if any account in the organization turns off the Block Public Access feature on an Amazon S3 bucket. A DevOps engineer must implement this change without affecting the operation of any AWS accounts. The implementation must ensure that individual member accounts in the organization cannot turn off the notification.

Which solution will meet these requirements?

A. Designate an account to be the delegated Amazon GuardDuty administrator account. Turn on GuardDuty for all accounts across the organization. In the GuardDuty administrator account, create an SNS topic. Subscribe the SecOps team\\'s email address to the SNS topic. In the same account, create an Amazon EventBridge rule that uses an event pattern for GuardDuty findings and a target of the SNS topic.

B. Create an AWS CloudFormation template that creates an SNS topic and subscribes the SecOps team\\'s email address to the SNS topic. In the template, include an Amazon EventBridge rule that uses an event pattern of CloudTrail activity for s3:PutBucketPublicAccessBlock and a target of the SNS topic. Deploy the stack to every account in the organization by using CloudFormation StackSets.

C. Turn on AWS Config across the organization. In the delegated administrator account, create an SNS topic. Subscribe the SecOps team\\'s email address to the SNS topic. Deploy a conformance pack that uses the s3-bucket-level-publicaccess-prohibited AWS Config managed rule in each account and uses an AWS Systems Manager document to publish an event to the SNS topic to notify the SecOps team.

D. Turn on Amazon Inspector across the organization. In the Amazon Inspector delegated administrator account, create an SNS topic. Subscribe the SecOps team\\'s email address to the SNS topic. In the same account, create an Amazon EventBridge rule that uses an event pattern for public network exposure of the S3 bucket and publishes an event to the SNS topic to notify the SecOps team.

Correct Answer: C

Amazon GuardDuty is primarily on threat detection and response, not configuration monitoring A conformance pack is a collection of AWS Config rules and remediation actions that can be easily deployed as a single entity in an account and a Region or across an organization in AWS Organizations.
https://docs.aws.amazon.com/config/latest/developerguide/conformance-packs.html
https://docs.aws.amazon.com/config/latest/developerguide/s3-account-level-public-access-blocks.html

QUESTION 2

A company builds an application that uses an Application Load Balancer in front of Amazon EC2 instances that are in an Auto Scaling group.

The application is stateless. The Auto Scaling group uses a custom AMI that is fully prebuilt.

The EC2 instances do not have a custom bootstrapping process.

The AMI that the Auto Scaling group uses was recently deleted.

The Auto Scaling group\\'s scaling activities show failures because the AMI ID does not exist.

Which combination of steps should a DevOps engineer take to meet these requirements? (Select THREE.)

A. Create a new launch template that uses the new AMI.

B. Update the Auto Scaling group to use the new launch template.

C. Reduce the Auto Scaling group\\'s desired capacity to O.

D. Increase the Auto Scaling group\\'s desired capacity by I.

E. Create a new AMI from a running EC2 instance in the Auto Scaling group.

F. Create a new AMI by copying the most recent public AMI of the operating system that the EC2 instances use.

Correct Answer: ABE

ABE are correct: means we need a new AMI image from a runnung EC2 instance C and D: irrelevant, auto Scaling group\\'s desired capacity has nothing to do here

F: This option doesnt make sense

QUESTION 3

A company is implementing an Amazon Elastic Container Service (Amazon ECS) cluster to run its workload. The company architecture will run multiple ECS services on the cluster. The architecture includes an Application Load Balancer on the front end and uses multiple target groups to route traffic.

A DevOps engineer must collect application and access logs. The DevOps engineer then needs to send the logs to an Amazon S3 bucket for near-real-time analysis.

Which combination of steps must the DevOps engineer take to meet these requirements? (Choose three.)

A. Download the Amazon CloudWatch Logs container instance from AWS. Configure this instance as a task. Update the application service definitions to include the logging task.

B. Install the Amazon CloudWatch Logs agent on the ECS instances. Change the logging driver in the ECS task definition to awslogs.

C. Use Amazon EventBridge to schedule an AWS Lambda function that will run every 60 seconds and will run the Amazon CloudWatch Logs create-export-task command. Then point the output to the logging S3 bucket.

D. Activate access logging on the ALB. Then point the ALB directly to the logging S3 bucket.

E. Activate access logging on the target groups that the ECS services use. Then send the logs directly to the logging S3 bucket.

F. Create an Amazon Kinesis Data Firehose delivery stream that has a destination of the logging S3 bucket. Then create an Amazon CloudWatch Logs subscription filter for Kinesis Data Firehose.

Correct Answer: BDF

https://docs.aws.amazon.com/AmazonECS/latest/developerguide/ecs-logging-monitoring.html

QUESTION 4

A company is running a number of internet-facing APIs that use an AWS Lambda authorizer to control access. A security team wants to be alerted when a large number of requests are failing authorization, as this may indicate API abuse. Given the magnitude of API requests, the team wants to be alerted only if the number of HTTP 403 Forbidden responses goes above 2% of overall API calls.

Which solution will accomplish this?

A. Use the default Amazon API Gateway 403Error and Count metrics sent to Amazon CloudWatch, and use metric math to create a CloudWatch alarm. Use the (403Error/Count)*100 mathematical expression when defining the alarm. Set the alarm threshold to be greater than 2.

B. Write a Lambda function that fetches the default Amazon API Gateway 403Error and Count metrics sent to Amazon CloudWatch, calculate the percentage of errors, then push a custom metric to CloudWatch named Custorn403Percent. Create a CloudWatch alarm based on this custom metric. Set the alarm threshold to be greater than 2.

C. Configure Amazon API Gateway to send custom access logs to Amazon CloudWatch Logs. Create a log filter to produce a custom metric for the HTTP 403 response code named Custom403Error. Use this custom metric and the default API Gateway Count metric sent to CloudWatch, and use metric match to create a CloudWatch alarm. Use the (Custom403Error/Count)*100 mathematical expression when defining the alarm. Set the alarm threshold to be greater than 2.

D. Configure Amazon API Gateway to enable custom Amazon CloudWatch metrics, enable the ALL_STATUS_CODE option, and define an APICustom prefix. Use CloudWatch metric math to create a CloudWatch alarm. Use the (APICustom403Error/Count)*100 mathematical expression when defining the alarm. Set the alarm threshold to be greater than 2.

Correct Answer: C

Reference: https://aws.amazon.com/blogs/compute/analyzing-api-gateway-custom-access-logs-for-custom-domain-names/

QUESTION 5

An ecommerce company uses a large number of Amazon Elastic Block Store (Amazon EBS) backed Amazon EC2 instances. To decrease manual work across all the instances, a DevOps engineer is tasked with automating restart actions when EC2 instance retirement events are scheduled.

How can this be accomplished?

A. Create a scheduled Amazon EventBridge rule to run an AWS Systems Manager Automation runbook that checks if any EC2 instances are scheduled for retirement once a week. If the instance is scheduled for retirement, the runbook will hibernate the instance.

B. Enable EC2 Auto Recovery on all of the instances. Create an AWS Config rule to limit the recovery to occur during a maintenance window only.

C. Reboot all EC2 instances during an approved maintenance window that is outside of standard business hours. Set up Amazon CloudWatch alarms to send a notification in case any instance is failing EC2 instance status checks.

D. Set up an AWS Health Amazon EventBridge rule to run AWS Systems Manager Automation runbooks that stop and start the EC2 instance when a retirement scheduled event occurs.

Correct Answer: D

D is correct: : these even occurs when the underlying infra that runs the instances needs to be repaired. To deal with this, just need to stop and start the instance to re-locate the instance to a different physical machine

A: Hibernate would not work for this scenario

B: This would also bring back the instance. However, AWS config rule cannot limit the recovery. It only reports, not actions

C: This option is a manual work, not automated one