DOP-C02 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

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

QUESTION 1

You are hosting multiple environments in multiple regions and would like to use Amazon Inspector for regular security assessments on your AWS resources across all regions. Which statement about Amazon Inspector\\'s operation across regions is true?

A. Amazon Inspector is a global service that is not region-bound. You can include AWS resources from multiple regions in the same assessment target.

B. Amazon Inspector is hosted within AWS regions behind a public endpoint. All regions are isolated from each other, and the telemetry and findings for all assessments performed within a region remain in that region and are not distributed by the service to other Amazon Inspector locations.

C. Amazon Inspector is hosted in each supported region. Telemetry data and findings are shared across regions to provide complete assessment reports.

D. Amazon Inspector is hosted in each supported region separately. You have to create assessment targets using the same name and tags in each region and Amazon Inspector will run against each assessment target in each region.

Correct Answer: B

At this time, Amazon Inspector supports assessment services for EC2 instances in only the following AWS regions:

US West (Oregon)

US East (N. Virginia)

EU (Ireland)

Asia Pacific (Seoul)

Asia Pacific (Mumbai)

Asia Pacific (Tokyo)

Asia Pacific (Sydney)

Amazon Inspector is hosted within AWS regions behind a public endpoint. All regions are isolated from each other, and the telemetry and findings for all assessments performed within a region remain in that region and are not distributed by

the service to other Amazon Inspector locations.

Reference:

https://docs.aws.amazon.com/inspector/latest/userguide/inspector_supported_os_regions.html#in%20spector_supported-regions

QUESTION 2

A company uses an organization in AWS Organizations to manage several AWS accounts that the company\\'s developers use. The company requires all data to be encrypted in transit.

Multiple Amazon S3 buckets that were created in developer accounts allow unencrypted connections. A DevOps

engineer must enforce encryption of data in transit for all existing S3 buckets that are created in accounts in the organization.

Which solution will meet these requirements?

A. Use AWS CloudFormation StackSets to deploy an AWS Network Firewall firewall to each account. Route all outbound requests from the AWS environment through the firewall. Deploy a policy to block access to all outbound requests on port 80.

B. Use AWS CloudFormation StackSets to deploy an AWS Network Firewall firewall to each account. Route all inbound requests to the AWS environment through the firewall. Deploy a policy to block access to all inbound requests on port

80.

C. Turn on AWS Config for the organization. Deploy a conformance pack that uses the s3-bucket-ssl-requests-only managed rule and an AWS Systems Manager Automation runbook. Use a runbook that adds a bucket policy statement to deny access to an S3 bucket when the value of the aws:SecureTransport condition key is false.

D. Turn on AWS Config for the organization. Deploy a conformance pack that uses the s3-bucket-ssl-requests-only managed rule and an AWS Systems Manager Automation runbook. Use a runbook that adds a bucket policy statement to deny access to an S3 bucket when the value of the s3:x-amz-server-side-encryption-aws-kms-key-id condition key is null.

Correct Answer: C

aws:SecureTransport condition this will be allowing only encrypted connections over HTTPS (TLS) --> THIS IS WHAT WE NEED

s3:x-amz-server-side-encryption-aws-kms-key-id --> To require that a particular AWS KMS key be used to encrypt the objects in a bucket. WE DON\\'T NEED THIS HERE!

QUESTION 3

A DevOps engineer has automated a web service deployment by using AWS CodePipeline with the following steps:

1) An AWS CodeBuild project compiles the deployment artifact and runs unit tests.

2) An AWS CodeDeploy deployment group deploys the web service to Amazon EC2 instances in the staging environment.

3) A CodeDeploy deployment group deploys the web service to EC2 instances in the production environment.

The quality assurance (QA) team requests permission to inspect the build artifact before the deployment to the production environment occurs.

The QA team wants to run an internal penetration testing tool to conduct manual tests. The tool will be invoked by a REST API call.

Which combination of actions should the DevOps engineer take to fulfill this request? (Choose two.)

A. Insert a manual approval action between the test actions and deployment actions of the pipeline.

B. Modify the buildspec.yml file for the compilation stage to require manual approval before completion.

C. Update the CodeDeploy deployment groups so that they require manual approval to proceed.

D. Update the pipeline to directly call the REST API for the penetration testing tool.

E. Update the pipeline to invoke an AWS Lambda function that calls the REST API for the penetration testing tool.

Correct Answer: AE

QUESTION 4

A company uses Amazon EC2 instances to host applications for its customers. Recently, the company\\'s support team has received EC2 scheduled maintenance notifications regarding its EC2 instances.

The support team wants to automatically perform a restart of any EC2 instances with a scheduled maintenance event before the scheduled date.

Which solution will meet these requirements while requiring the MINIMUM amount of development effort?

A. Create an AWS Systems Manager maintenance window with a Systems Manager Automation tast that uses the RebootInstnaces EC2 API operation to restart the affected EC2 instances. Attach the EC2 instances to the maintenance window. Configure AWS Health to invoke the maintenance window whenever a scheduledChange event for Amazon EC2 is generated.

B. Create an Amazon CloudWatch alarm for the StatusCheckFailed metric of each EC2 instance. Configure the CloudWatch alarm to recover any affected EC2 instance.

C. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that matches scheduledChange events for Amazon EC2 from AWS Health. Configure the rule to run the AWS-RestartEC2Instance AWS Systems Manager Automation runbook.

D. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that matches scheduledChange events for Amazon EC2 from AWS Health. Create an AWS Lambda function that uses the EC2 API to list all EC2 instances with scheduled events and then uses the RebootInstances EC2 API operation to restart the affected EC2 instances. Configure the EventBridge (CloudWatch Events) rule to invoke the Lambda function.

Correct Answer: A

QUESTION 5

A DevOps team uses AWS CodePipeline, AWS CodeBuild, and AWS CodeDeploy to deploy an application. The application is a REST API that uses AWS Lambda functions and Amazon API Gateway Recent deployments have introduced errors that have affected many customers.

The DevOps team needs a solution that reverts to the most recent stable version of the application when an error is detected. The solution must affect the fewest customers possible.

Which solution Will meet these requirements With the MOST operational efficiency?

A. Set the deployment configuration in CodeDeploy to LambdaAllAtOnce Configure automatic rollbacks on the deployment group Create an Amazon CloudWatch alarm that detects HTTP Bad Gateway errors on API Gateway Configure the deployment group to roll back when the number of alarms meets the alarm threshold

B. Set the deployment configuration in CodeDeploy to LambdaCanary10Percent10Minutes. Configure automatic

rollbacks on the deployment group Create an Amazon CloudWatch alarm that detects HTTP Bad Gateway errors on API Gateway Configure the deployment group to roll back when the number of alarms meets the

alarm threshold

C. Set the deployment configuration in CodeDeploy to LambdaAllAtOnce Configure manual rollbacks on the deployment group. Create an Amazon Simple Notification Service (Amazon SNS) topc to send notifications every time a deployrnent fads. Configure the SNS topc to Invoke a new Lambda function that stops the current deployment and starts the most recent successful deployment

D. Set the deployment configuration in CodeDeploy to LambdaCanaryIOPercentIOMinutes Configure manual rollbacks on the deployment group Create a metric filter on an Amazon CloudWatch log group for API Gateway to monitor HTTP Bad Gateway errors. Configure the metric filter to Invoke a new Lambda function that stops the current eployment and starts the most recent successful deployment

Correct Answer: B

Option A is incorrect because setting the deployment configuration to LambdaAllAtOnce means that the new version of the application will be deployed to all Lambda functions at once, affecting all customers. This does not meet the requirement of affecting the fewest customers possible. Moreover, configuring automatic rollbacks on the deployment group is not operationally efficient, as it requires manual intervention to fix the errors and redeploy the application. Option B is correct because setting the deployment configuration to LambdaCanary10Percent10Minutes means that the new version of the application will be deployed to 10 percent of the Lambda functions first, and then to the remaining 90 percent after 10 minutes. This minimizes the impact of errors on customers, as only 10 percent of them will be affected by a faulty deployment. Configuring automatic rollbacks on the deployment group also meets the requirement of reverting to the most recent stable version of the application when an error is detected. Creating a CloudWatch alarm that detects HTTP Bad Gateway errors on API Gateway is a valid way to monitor the health of the application and trigger a rollback if needed. Option C is incorrect because setting the deployment configuration to LambdaAllAtOnce means that the new version of the application will be deployed to all Lambda functions at once, affecting all customers. This does not meet the requirement of affecting the fewest customers possible. Moreover, configuring manual rollbacks on the deployment group is not operationally efficient, as it requires human intervention to stop the current deployment and start a new one. Creating an SNS topic to send notifications every time a deployment fails is not sufficient to detect errors in the application, as it does not monitor the API Gateway responses. Option D is incorrect because configuring manual rollbacks on the deployment group is not operationally efficient, as it requires human intervention to stop the current deployment and start a new one. Creating a metric filter on a CloudWatch log group for API Gateway to monitor HTTP Bad Gateway errors is a valid way to monitor the health of the application, but invoking a new Lambda function to perform a rollback is unnecessary and complex, as CodeDeploy already provides automatic rollback functionality. References: AWS CodeDeploy Deployment Configurations [AWS CodeDeploy Rollbacks] Amazon CloudWatch Alarms