# Free Questions for SOA-C02 by vceexamstest

## Shared by Coleman on 09-08-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

A company runs us Infrastructure on Amazon EC2 Instances that run In an Auto Scaling group. Recently, the company promoted faulty code to the entire EC2 fleet. This faulty code caused the Auto Scaling group to scale the instances before any of the application logs could be retrieved.

What should a SysOps administrator do to retain the application logs after instances are terminated?

A Configure an Auto Scaling lifecycle hook to create a snapshot of the ephemeral storage upon termination of the instances.

## Options:

**B)** Create a new Amazon Machine Image (AMI) that has the Amazon CloudWatch agent installed and configured to send logs to Amazon CloudWatch Logs. Update the launch template to use the new AMI.

**C)** Create a new Amazon Machine Image (AMI) that has a custom script configured to send logs to AWS CloudTrail. Update the launch template to use the new AMI.

**D)** Install the Amazon CloudWatch agent on the Amazon Machine Image (AMI) that is defined in the launch template. Configure the CloudWatch agent to back up the logs to ephemeral storage.

## Answer:

B

# Question 2

**Question Type:** MultipleChoice

A company has a compliance requirement that no security groups can allow SSH ports to be open to all IP addresses. A SysOps administrator must implement a solution that will notify the company's SysOps team when a security group rule violates this requirement. The solution also must remediate the security group rule automatically.

Which solution will meet these requirements?

AZ. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function when a security group changes. Configure the Lambda function to evaluate the security group for compliance, remove all inbound security group rules on all ports, and notify the SysOps team if the security group is noncompliant.

## Options:

**B)** Create an AWS CloudTrail metric filter for security group changes. Create an Amazon CloudWatch alarm to notify the SysOps team through an Amazon Simple Notification Service (Amazon SNS) topic when (he metric is greater than 0. Subscribe an AWS Lambda function to the SNS topic to remediate the security group rule by removing the rule.

**C)** Activate the AWS Config restricted-ssh managed rule. Add automatic remediation to the AWS Config rule by using the AWS Systems Manager Automation AWS-
DisablePublicAccessForSecurityGroup runbook. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to notify the

SysOps team when the rule is noncompliant.

**D)** Create an AWS CloudTrail metric filter for security group changes. Create an Amazon CloudWatch alarm for when the metric is greater than 0. Add an AWS Systems Manager action to the CloudWatch alarm to suspend the security group by using the Systems Manager Automation AWS-DisablePublicAccessForSecurityGroup runbook when the alarm is in ALARM state. Add an Amazon Simple Notification Service (Amazon SNS) topic as a second target to notify the SysOps team.

### Answer:

C

# Question 3

**Question Type:** MultipleChoice

A new website will run on Amazon EC2 instances behind an Application Load Balancer. Amazon Route 53 will be used to manage DNS records.

What type of record should be set in Route 53 to point the website's apex domain name (for example, "company.com") to the Application Load Balancer?

### Options:

**A)** CNAME

**B)** SOA

**C)** TXT

**D)** ALIAS

### Answer:

D

# Question 4

**Question Type:** MultipleChoice

A company is using an AWS KMS customer master key (CMK) with imported key material The company Reference the CMK by its alias in the Java application to encrypt data The CMK must be rotated every 6 months

What is the process to rotate the key?

### Options:

**A)** Enable automatic key rotation for the CMK and specify a period of 6 months

**B)** Create a new CMK with new imported material, and update the key alias to point to the new CMK.

**C)** Delete the current key material, and import new material into the existing CMK

**D)** Import a copy of the existing key material into a new CMK as a backup, and set the rotation schedule for 6 months

### Answer:

B

# Question 5

**Question Type:** MultipleChoice

A SysOps administrator is notified that an Amazon EC2 instance has stopped responding. The AWS

Management Console indicates that the system checks are failing.

What should the administrator do first to resolve this issue?

### Options:

**A)** Reboot the EC2 instance so it can be launched on a new host.

**B)** Stop and then start the EC2 instance so that it can be launched on a new host.

**C)** Terminate the EC2 instance and relaunch it.

**D)** View the AWS CloudTrail log to investigate what changed on the EC2 instance.

### Answer:

B

# Question 6

**Question Type:** MultipleChoice

A company has an infernal web application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone. A SysOps administrator must make the application highly available.

Which action should the SysOps administrator take to meet this requirement?

### Options:

**A)** Increase the maximum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.

**B)** Increase the minimum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.

**C)** Update the Auto Scaling group to launch new instances in a second Availability Zone in the same AWS Region.

**D)** Update the Auto Scaling group to launch new instances in an Availability Zone in a second AWS Region.

### Answer:

C

# Question 7

**Question Type:** **MultipleChoice**

update an existing AWS CloudFormation stack. If needed, a copy 0t the CloudFormation template is available in an Amazon SB bucket named cloudformation-bucket

1. Use the us-east-2 Region for all resources.

2. Unless specified below, use the default configuration settings.

3. update the Amazon EQ instance named Devinstance by making the following changes to the stack named 1700182:

a) Change the EC2 instance type to us-east-t2.nano.

b) Allow SSH to connect to the EC2 instance from the IP address range

192.168.100.0/30.

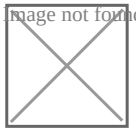
c) Replace the instance profile IAM role with IamRoleB.

4. Deploy the changes by updating the stack using the CFServiceR01e role.

5. Edit the stack options to prevent accidental deletion.

6. Using the output from the stack, enter the value of the ProdInstanceId in the text box below:

Image not found or type unknown



## Options:

**A)** Explanation:

Solution as given below.

Image not found or type unknown

## Answer:

A

# Question 8

**Question Type:** MultipleChoice

If your AWS Management Console browser does not show that you are logged in to an AWS account, close the browser and relaunch the

console by using the AWS Management Console shortcut from the VM desktop.

If the copy-paste functionality is not working in your environment, refer to the instructions file on the VM desktop and use Ctrl+C, Ctrl+V or Command-C , Command-V.

Configure Amazon EventBridge to meet the following requirements.

1. use the us-east-2LRegion for all resources,

2. Unless specified below, use the default configuration settings.

3. Use your own resource naming unless a resource

name is specified below.

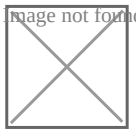
4. Ensure all Amazon EC2 events in the default event

bus are replayable for the past 90 days.

5. Create a rule named RunFunction to send the exact message every 1 5 minutes to an existing AWS Lambda function named LogEventFunction.

6. Create a rule named SpotWarning to send a notification to a new standard Amazon SNS topic named TopicEvents whenever an Amazon EC2

Spot Instance is interrupted. Do NOT create any topic subscriptions. The notification must match the following structure:



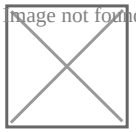

Input template:

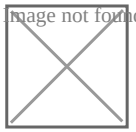
" The EC2 Spot Instance <instance> has been on account.

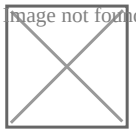
## Options:

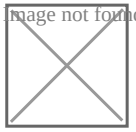
**A)** Explanation:

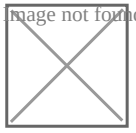
Solution as given below.

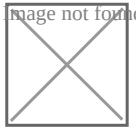





### Answer:

A

# Question 9

**Question Type:** **MultipleChoice**

An Amazon S3 Inventory report reveals that more than 1 million objects in an S3 bucket are not encrypted.

These objects must be encrypted, and all future objects must be encrypted at the time they are written.

Which combination of actions should a SysOps administrator take to meet these requirements? (Choose two.)

## Options:

**A)** Create an AWS Config rule that runs evaluations against configuration changes to the S3 bucket. When an unencrypted object is found, run an AWS Systems Manager Automation document to encrypt the object in place.

**B)** Edit the properties of the S3 bucket to enable default server-side encryption.

**C)** Filter the S3 Inventory report by using S3 Select to find all objects that are not encrypted. Create an S3 Batch Operations job to copy each object in place with encryption enabled.

**D)** Filter the S3 Inventory report by using S3 Select to find all objects that are not encrypted. Send each object name as a message to an Amazon Simple Queue Service (Amazon SQS) queue. Use the SQS queue to invoke an AWS Lambda function to tag each object with a key of 'Encryption' and a value of 'SSE-KMS'.

**E)** Use S3 Event Notifications to invoke an AWS Lambda function on all new object-created events for the S3 bucket. Configure the Lambda function to check whether the object is encrypted and to run an AWS Systems Manager Automation document to encrypt the object in place when an unencrypted object is found.

## Answer:

B, E

# Question 10

**Question Type:** MultipleChoice

A company runs us Infrastructure on Amazon EC2 Instances that run In an Auto Scaling group. Recently, the company promoted faulty code to the entire EC2 fleet. This faulty code caused the Auto Scaling group to scale the instances before any of the application logs could be retrieved.

What should a SysOps administrator do to retain the application logs after instances are terminated?

A Configure an Auto Scaling lifecycle hook to create a snapshot of the ephemeral storage upon termination of the instances.

## Options:

**B)** Create a new Amazon Machine Image (AMI) that has the Amazon CloudWatch agent installed and configured to send logs to Amazon CloudWatch Logs. Update the launch template to use the new AMI.

**C)** Create a new Amazon Machine Image (AMI) that has a custom script configured to send logs to AWS CloudTrail. Update the launch template to use the new AMI.

**D)** Install the Amazon CloudWatch agent on the Amazon Machine Image (AMI) that is defined in the launch template. Configure the CloudWatch agent to back up the logs to ephemeral storage.

## Answer:

B

# Question 11

**Question Type:** MultipleChoice

A company has a compliance requirement that no security groups can allow SSH ports to be open to all IP addresses. A SysOps administrator must implement a solution that will notify the company's SysOps team when a security group rule violates this requirement. The solution also must remediate the security group rule automatically.

Which solution will meet these requirements?

AZ. Create an Amazon EventBridge (Amazon CloudWatch Events) rule that invokes an AWS Lambda function when a security group changes. Configure the Lambda function to evaluate the security group for compliance, remove all inbound security group rules on all ports, and notify the SysOps team if the security group is noncompliant.

## Options:

**B)** Create an AWS CloudTrail metric filter for security group changes. Create an Amazon CloudWatch alarm to notify the SysOps team through an Amazon Simple Notification Service (Amazon SNS) topic when (he metric is greater than 0. Subscribe an AWS Lambda function to the SNS topic to remediate the security group rule by removing the rule.

**C)** Activate the AWS Config restricted-ssh managed rule. Add automatic remediation to the AWS Config rule by using the AWS Systems Manager Automation AWS-
DisablePublicAccessForSecurityGroup runbook. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to notify the

SysOps team when the rule is noncompliant.

**D)** Create an AWS CloudTrail metric filter for security group changes. Create an Amazon CloudWatch alarm for when the metric is greater than 0. Add an AWS Systems Manager action to the CloudWatch alarm to suspend the security group by using the Systems Manager Automation AWS-DisablePublicAccessForSecurityGroup runbook when the alarm is in ALARM state. Add an Amazon Simple Notification Service (Amazon SNS) topic as a second target to notify the SysOps team.

## Answer:

C