SCS-C02 Q&As

AWS Certified Security - Specialty

Pass Amazon SCS-C02 Exam with 100% Guarantee

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

https://www.passapply.com/scs-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

A company has recently recovered from a security incident that required the restoration of Amazon EC2 instances from snapshots.

After performing a gap analysis of its disaster recovery procedures and backup strategies, the company is concerned that, next time, it will not be able to recover the EC2 instances if the AWS account was compromised and Amazon EBS

snapshots were deleted.

All EBS snapshots are encrypted using an AWS KMS CMK.

Which solution would solve this problem?

A. Create a new Amazon S3 bucket. Use EBS lifecycle policies to move EBS snapshots to the new S3 bucket. Move snapshots to Amazon S3 Glacier using lifecycle policies, and apply Glacier Vault Lock policies to prevent deletion.

B. Use AWS Systems Manager to distribute a configuration that performs local backups of all attached disks to Amazon S3.

C. Create a new AWS account with limited privileges. Allow the new account to access the AWS KMS key used to encrypt the EBS snapshots, and copy the encrypted snapshots to the new account on a recurring basis.

D. Use AWS Backup to copy EBS snapshots to Amazon S3.

Correct Answer: C

This answer is correct because creating a new AWS account with limited privileges would provide an isolated and secure backup destination for the EBS snapshots. Allowing the new account to access the AWS KMS key used to encrypt the EBS snapshots would enable cross-account snapshot sharing without requiring re-encryption. Copying the encrypted snapshots to the new account on a recurring basis would ensure that the backups are up-to-date and consistent.

QUESTION 2

A company needs to encrypt all of its data stored in Amazon S3. The company wants to use IAM Key Management Service (IAM KMS) to create and manage its encryption keys. The company\\'s security policies require the ability to Import the company\\'s own key material for the keys, set an expiration date on the keys, and delete keys immediately, if needed.

How should a security engineer set up IAM KMS to meet these requirements?

A. Configure IAM KMS and use a custom key store. Create a customer managed CMK with no key material Import the company\\'s keys and key material into the CMK

B. Configure IAM KMS and use the default Key store Create an IAM managed CMK with no key material Import the company\\'s key material into the CMK

C. Configure IAM KMS and use the default key store Create a customer managed CMK with no key material import the company\\'s key material into the CMK

D. Configure IAM KMS and use a custom key store. Create an IAM managed CMK with no key material. Import the company\\'s key material into the CMK.

Correct Answer: A

To meet the requirements of importing their own key material, setting an expiration date on the keys, and deleting keys immediately, the security engineer should do the following:

Configure AWS KMS and use a custom key store. This allows the security engineer to use a key manager outside of AWS KMS that they own and manage, such as an AWS CloudHSM cluster or an external key manager. Create a customer

managed CMK with no key material. Import the company\\'s keys and key material into the CMK. This allows the security engineer to use their own key material for encryption and decryption operations, and to specify an expiration date for it.

QUESTION 3

A company uses AWS Organizations to manage a multi-accountAWS environment in a single AWS Region. The organization\\'s management account is named management-01. The company has turned on AWS Config in all accounts in the organization. The company has designated an account named security-01 as the delegated administrator for AWS Config.

All accounts report the compliance status of each account\\'s rules to the AWS Config delegated administrator account by using an AWS Config aggregator. Each account administrator can configure and manage the account\\'s own AWS Config rules to handle each account\\'s unique compliance requirements.

A security engineer needs to implement a solution to automatically deploy a set of 10 AWS Config rules to all existing and future AWS accounts in the organiza-tion. The solution must turn on AWS Config automatically during account creation.

Which combination of steps will meet these requirements? (Select TWO.)

A. Create an AWS CloudFormation template that contains the 1 0 required AVVS Config rules. Deploy the template by using CloudFormation StackSets in the security-01 account.

B. Create a conformance pack that contains the 10 required AWS Config rules. Deploy the conformance pack from the security-01 account.

C. Create a conformance pack that contains the 10 required AWS Config rules. Deploy the conformance pack from the management-01 account.

D. Create an AWS CloudFormation template that will activate AWS Config. De-ploy the template by using CloudFormation StackSets in the security-01 ac-count.

E. Create an AWS CloudFormation template that will activate AWS Config. De-ploy the template by using CloudFormation StackSets in the management-01 account.

Correct Answer: BE

QUESTION 4

A security engineer receives an IAM abuse email message. According to the message, an Amazon EC2 instance that is running in the security engineer\\'s IAM account is sending phishing email messages.

The EC2 instance is part of an application that is deployed in production. The application runs on many EC2 instances

behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group across multiple subnets and multiple Availability Zones.

The instances normally communicate only over the HTTP. HTTPS, and MySQL protocols. Upon investigation, the security engineer discovers that email messages are being sent over port 587. All other traffic is normal.

The security engineer must create a solution that contains the compromised EC2 instance, preserves forensic evidence for analysis, and minimizes application downtime. Which combination of steps must the security engineer take to meet these requirements? (Select THREE.)

A. Add an outbound rule to the security group that is attached to the compromised EC2 instance to deny traffic to 0.0.0.0/0 and port 587.

B. Add an outbound rule to the network ACL for the subnet that contains the compromised EC2 instance to deny traffic to 0.0.0.0/0 and port 587.

C. Gather volatile memory from the compromised EC2 instance. Suspend the compromised EC2 instance from the Auto Scaling group. Then take a snapshot of the compromised EC2 instance.

D. Take a snapshot of the compromised EC2 instance. Suspend the compromised EC2 instance from the Auto Scaling group. Then gather volatile memory from the compromised EC2 instance.

E. Move the compromised EC2 instance to an isolated subnet that has a network ACL that has no inbound rules or outbound rules.

F. Replace the existing security group that is attached to the compromised EC2 instance with a new security group that has no inbound rules or outbound rules.

Correct Answer: ACE

QUESTION 5

A security engineer is creating an AWS Lambda function. The Lambda function needs to use a role that is named LambdaAuditRole to assume a role that is named AcmeAuditFactoryRole in a different AWS account.

When the code is processed, the following error message appears: "An error oc-curred (AccessDenied) when calling the AssumeRole operation."

Which combination of steps should the security engineer take to resolve this er-ror? (Select TWO.)

A. Ensure that LambdaAuditRole has the sts:AssumeRole permission for Ac-meAuditFactoryRole.

B. Ensure that LambdaAuditRole has the AWSLambdaBasicExecutionRole managed policy attached.

C. Ensure that the trust policy for AcmeAuditFactoryRole allows the sts:AssumeRole action from LambdaAuditRole.

D. Ensure that the trust policy for LambdaAuditRole allows the sts:AssumeRole action from the lambda.amazonaws.com service.

E. Ensure that the sts:AssumeRole API call is being issued to the us-east-I Region endpoint.

Correct Answer: AC

SCS-C02 PDF Dumps SCS-C02 VCE Dumps SCS-C02 Study Guide