



Amazon-Web-Services

Exam Questions SCS-C03

AWS Certified Security - Specialty

NEW QUESTION 1

A security team manages a company's AWS Key Management Service (AWS KMS) customer managed keys. Only members of the security team can administer the KMS keys. The company's application team has a software process that needs temporary access to the keys occasionally. The security team needs to provide the application team's software process with access to the keys.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Export the KMS key material to an on-premises hardware security module (HSM). Give the application team access to the key material.
- B. Edit the key policy that grants the security team access to the KMS keys by adding the application team as principal
- C. Revert this change when the application team no longer needs access.
- D. Create a key grant to allow the application team to use the KMS key
- E. Revoke the grant when the application team no longer needs access.
- F. Create a new KMS key by generating key material on premise
- G. Import the key material to AWS KMS whenever the application team needs access
- H. Grant the application team permissions to use the key.

Answer: C

NEW QUESTION 2

A company stores sensitive data in an Amazon S3 bucket. The company encrypts the data at rest by using server-side encryption with Amazon S3 managed keys (SSE-S3). A security engineer must prevent any modifications to the data in the S3 bucket.

Which solution will meet this requirement?

- A. Configure S3 bucket policies to deny DELETE and PUT object permissions.
- B. Configure S3 Object Lock in compliance mode with S3 bucket versioning enabled.
- C. Change the encryption on the S3 bucket to use AWS Key Management Service (AWS KMS) customer managed keys.
- D. Configure the S3 bucket with multi-factor authentication (MFA) delete protection.

Answer: B

NEW QUESTION 3

A company's security team wants to receive near-real-time email notifications about AWS abuse reports related to DoS attacks. An Amazon SNS topic already exists and is subscribed to by the security team.

What should the security engineer do next?

- A. Poll Trusted Advisor for abuse notifications by using a Lambda function.
- B. Create an Amazon EventBridge rule that matches AWS Health events for AWS_ABUSE_DOS_REPORT and publishes to SNS.
- C. Poll the AWS Support API for abuse cases by using a Lambda function.
- D. Detect abuse reports by using CloudTrail logs and CloudWatch alarms.

Answer: B

NEW QUESTION 4

A company is attempting to conduct forensic analysis on an Amazon EC2 instance, but the company is unable to connect to the instance by using AWS Systems Manager Session Manager. The company has installed AWS Systems Manager Agent (SSM Agent) on the EC2 instance.

The EC2 instance is in a subnet in a VPC that does not have an internet gateway attached. The company has associated a security group with the EC2 instance. The security group does not have inbound or outbound rules. The subnet's network ACL allows all inbound and outbound traffic.

Which combination of actions will allow the company to conduct forensic analysis on the EC2 instance without compromising forensic data? (Select THREE.)

- A. Update the EC2 instance security group to add a rule that allows outbound traffic on port 443 for 0.0.0.0/0.
- B. Update the EC2 instance security group to add a rule that allows inbound traffic on port 443 to the VPC's CIDR range.
- C. Create an EC2 key pair
- D. Associate the key pair with the EC2 instance.
- E. Create a VPC interface endpoint for Systems Manager in the VPC where the EC2 instance is located.
- F. Attach a security group to the VPC interface endpoint
- G. Allow inbound traffic on port 443 to the VPC's CIDR range.
- H. Create a VPC interface endpoint for the EC2 instance in the VPC where the EC2 instance is located.

Answer: ADE

NEW QUESTION 5

A company has decided to move its fleet of Linux-based web server instances to an Amazon EC2 Auto Scaling group. Currently, the instances are static and are launched manually. When an administrator needs to view log files, the administrator uses SSH to establish a connection to the instances and retrieves the logs manually.

The company often needs to query the logs to produce results about application sessions and user issues. The company does not want its new automatically scaling architecture to result in the loss of any log files when instances are scaled in.

Which combination of steps should a security engineer take to meet these requirements MOST cost-effectively? (Select TWO.)

- A. Configure a cron job on the instances to forward the log files to Amazon S3 periodically.
- B. Configure AWS Glue and Amazon Athena to query the log files.
- C. Configure the Amazon CloudWatch agent on the instances to forward the logs to Amazon CloudWatch Logs.
- D. Configure Amazon CloudWatch Logs Insights to query the log files.
- E. Configure the instances to write the logs to an Amazon Elastic File System (Amazon EFS) volume.

Answer: CD

NEW QUESTION 6

A company wants to establish separate AWS Key Management Service (AWS KMS) keys to use for different AWS services. The company's security engineer created a key policy to allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructureDeployment IAM role. The security engineer recently discovered that IAM roles other than the InfrastructureDeployment role used this key for other services.

Which change to the policy should the security engineer make to resolve these issues?

- A. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change StringEquals to StringLike.
- B. In the policy document, remove the statement block that contains the Sid "Enable IAM User Permissions". Add key management policies to the KMS policy.
- C. In the statement block that contains the Sid "Allow use of the key", under the "Condition" block, change the kms:ViaService value to ec2.us-east-1.amazonaws.com.
- D. In the policy document, add a new statement block that grants the kms:Disable* permission to the security engineer's IAM role.

Answer: C

NEW QUESTION 7

An AWS Lambda function was misused to alter data, and a security engineer must identify who invoked the function and what output was produced. The engineer cannot find any logs created by the Lambda function in Amazon CloudWatch Logs.

Which of the following explains why the logs are not available?

- A. The execution role for the Lambda function did not grant permissions to write log data to CloudWatch Logs.
- B. The Lambda function was invoked by using Amazon API Gateway, so the logs are not stored in CloudWatch Logs.
- C. The execution role for the Lambda function did not grant permissions to write to the Amazon S3 bucket where CloudWatch Logs stores the logs.
- D. The version of the Lambda function that was invoked was not current.

Answer: A

NEW QUESTION 8

A company uses AWS IAM Identity Center with SAML 2.0 federation. The company decides to change its federation source from one identity provider (IdP) to another. The underlying directory for both IdPs is Active Directory.

Which solution will meet this requirement?

- A. Disable all existing users and groups within IAM Identity Center that were part of the federation with the original IdP.
- B. Modify the attribute mappings within the IAM Identity Center trust relationship to match information that the new IdP sends.
- C. Reconfigure all existing IAM roles in the company's AWS accounts to explicitly trust the new IdP as the principal.
- D. Confirm that the Network Time Protocol (NTP) clock skew is correctly set between IAM Identity Center and the new IdP endpoints.

Answer: B

NEW QUESTION 9

A company has a single AWS account and uses an Amazon EC2 instance to test application code. The company recently discovered that the instance was compromised and was serving malware. Analysis showed that the instance was compromised 35 days ago. A security engineer must implement a continuous monitoring solution that automatically notifies the security team by email for high severity findings as soon as possible.

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

- A. Enable AWS Security Hub in the AWS account.
- B. Enable Amazon GuardDuty in the AWS account.
- C. Create an Amazon Simple Notification Service (Amazon SNS) topic.
- D. Subscribe the security team's email distribution list to the topic.
- E. Create an Amazon Simple Queue Service (Amazon SQS) queue.
- F. Subscribe the security team's email distribution list to the queue.
- G. Create an Amazon EventBridge rule for GuardDuty findings of high severity.
- H. Configure the rule to publish a message to the topic.
- I. Create an Amazon EventBridge rule for Security Hub findings of high severity.
- J. Configure the rule to publish a message to the queue.

Answer: BCE

NEW QUESTION 10

A company requires a specific software application to be installed on all new and existing Amazon EC2 instances across an AWS Organization. SSM Agent is installed and active.

How can the company continuously monitor deployment status of the software application?

- A. Use AWS Config organization-wide with the ec2-managedinstance-applications-required managed rule and specify the application name.
- B. Use approved AMIs rule organization-wide.
- C. Use Distributor package and review output.
- D. Use Systems Manager Application Manager inventory filtering.

Answer: A

NEW QUESTION 10

A company is using AWS CloudTrail and Amazon CloudWatch to monitor resources in an AWS account. The company's developers have been using an IAM role in the account for the last 3 months.

A security engineer needs to refine the customer managed IAM policy attached to the role to ensure that the role provides least privilege access.

Which solution will meet this requirement with the LEAST effort?

- A. Implement AWS IAM Access Analyzer policy generation on the role.
- B. Implement AWS IAM Access Analyzer policy validation on the role.
- C. Search CloudWatch logs to determine the actions the role invoked and to evaluate the permissions.

D. Use AWS Trusted Advisor to compare the policies assigned to the role against AWS best practices.

Answer: A

NEW QUESTION 13

A company has a PHP-based web application that uses Amazon S3 as an object store for user files. The S3 bucket is configured for server-side encryption with Amazon S3 managed keys (SSE-S3). New requirements mandate full control of encryption keys. Which combination of steps must a security engineer take to meet these requirements? (Select THREE.)

- A. Create a new customer managed key in AWS Key Management Service (AWS KMS).
- B. Change the SSE-S3 configuration on the S3 bucket to server-side encryption with customer-provided keys (SSE-C).
- C. Configure the PHP SDK to use the SSE-S3 key before upload.
- D. Create an AWS managed key for Amazon S3 in AWS KMS.
- E. Change the SSE-S3 configuration on the S3 bucket to server-side encryption with AWS KMS managed keys (SSE-KMS).
- F. Change all the S3 objects in the bucket to use the new encryption key.

Answer: AEF

NEW QUESTION 14

A company must immediately disable compromised IAM users across all AWS accounts and collect all actions performed by the user in the last 7 days. Which solution will meet these requirements?

- A. Disable the IAM user and query CloudTrail logs in Amazon S3 using Athena.
- B. Remove IAM policies and query logs in Security Hub.
- C. Remove permission sets and query logs using CloudWatch Logs Insights.
- D. Disable the user in IAM Identity Center and query the organizational event data store.

Answer: D

NEW QUESTION 18

A company must capture AWS CloudTrail data events and must retain the logs for 7 years. The logs must be immutable and must be available to be searched by complex queries. The company also needs to visualize the data from the logs. Which solution will meet these requirements MOST cost-effectively?

- A. Create a CloudTrail Lake data store.
- B. Implement CloudTrail Lake dashboards to visualize and query the results.
- C. Use the CloudTrail Event History feature in the AWS Management Console.
- D. Visualize and query the results in the console.
- E. Send the CloudTrail logs to an Amazon S3 bucket.
- F. Provision a persistent Amazon EMR cluster that has access to the S3 bucket.
- G. Enable S3 Object Lock on the S3 bucket.
- H. Use Apache Spark to perform queries.
- I. Use Amazon QuickSight for visualizations.
- J. Send the CloudTrail logs to a log group in Amazon CloudWatch Logs.
- K. Set the CloudWatch Logs stream to send the data to an Amazon OpenSearch Service domain.
- L. Enable cold storage for the OpenSearch Service domain.
- M. Use OpenSearch Dashboards for visualizations and queries.

Answer: A

NEW QUESTION 21

A company sends Apache logs from EC2 Auto Scaling instances to a CloudWatch Logs log group with 1-year retention. A suspicious IP address appears in logs. A security engineer needs to analyze the past week of logs to count requests from that IP and list requested URLs. What should the engineer do with the LEAST effort?

- A. Export to S3 and use Macie.
- B. Stream to OpenSearch and analyze.
- C. Use CloudWatch Logs Insights with queries.
- D. Export to S3 and use AWS Glue.

Answer: C

NEW QUESTION 23

A security engineer needs to implement a solution to identify any sensitive data that is stored in an Amazon S3 bucket. The solution must report on sensitive data in the S3 bucket by using an existing Amazon Simple Notification Service (Amazon SNS) topic. Which solution will meet these requirements with the LEAST implementation effort?

- A. Enable AWS Config.
- B. Configure AWS Config to monitor for sensitive data in the S3 bucket and to send notifications to the SNS topic.
- C. Create an AWS Lambda function to scan the S3 bucket for sensitive data that matches a pattern.
- D. Program the Lambda function to send notifications to the SNS topic.
- E. Configure Amazon Macie to use managed data identifiers to identify and categorize sensitive data.
- F. Create an Amazon EventBridge rule to send notifications to the SNS topic.
- G. Enable Amazon GuardDuty.
- H. Configure AWS CloudTrail S3 data event.
- I. Create an Amazon CloudWatch alarm that reacts to GuardDuty findings and sends notifications to the SNS topic.

Answer: C

NEW QUESTION 25

A company uploads data files as objects into an Amazon S3 bucket. A vendor downloads the objects to perform data processing. A security engineer must implement a solution that prevents objects from residing in the S3 bucket for longer than 72 hours.

- A. Configure S3 Versioning to expire object versions that have been in the bucket for 72 hours.
- B. Configure an S3 Lifecycle configuration rule on the bucket to expire objects after 72 hours.
- C. Use the S3 Intelligent-Tiering storage class and configure expiration after 72 hours.
- D. Generate presigned URLs that expire after 72 hours.

Answer: B

NEW QUESTION 27

A company has a web application that reads from and writes to an Amazon S3 bucket. The company needs to authenticate all S3 API calls with AWS credentials. Which solution will provide the application with AWS credentials?

- A. Use Amazon Cognito identity pools and the GetId API.
- B. Use Amazon Cognito identity pools and AssumeRoleWithWebIdentity.
- C. Use Amazon Cognito user pools with ID tokens.
- D. Use Amazon Cognito user pools with access tokens.

Answer: B

NEW QUESTION 32

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

SCS-C03 Practice Exam Features:

- * SCS-C03 Questions and Answers Updated Frequently
- * SCS-C03 Practice Questions Verified by Expert Senior Certified Staff
- * SCS-C03 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * SCS-C03 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SCS-C03 Practice Test Here](#)