



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 a legacy application that runs on a single Amazon EC2 instance. A security audit shows that the application has been using an IAM access key within its code to access an Amazon S3 bucket that is named DOC-EXAMPLEBUCKET1 in the same AWS account. This access key pair has the s3:GetObject permission to all objects in only this S3 bucket. The company takes the application offline because the application is not compliant with the company's security policies for accessing other AWS resources from Amazon EC2. A security engineer validates that AWS CloudTrail is turned on in all AWS Regions. CloudTrail is sending logs to an S3 bucket that is named DOC-EXAMPLE-BUCKET2. This S3 bucket is in the same AWS account as DOC-EXAMPLEBUCKET1. However, CloudTrail has not been configured to send logs to Amazon CloudWatch Logs.

The company wants to know if any objects in DOC-EXAMPLE-BUCKET1 were accessed with the IAM access key in the past 60 days. If any objects were accessed, the company wants to know if any of the objects that are text files (.txt extension) contained personally identifiable information (PII).

Which combination of steps should the security engineer take to gather this information? (Choose two.)

- A. Configure Amazon Macie to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.
- B. Use Amazon CloudWatch Logs Insights to identify any objects in DOC-EXAMPLE-BUCKET1 that contain PII and that were available to the access key.
- C. Use Amazon OpenSearch Service (Amazon Elasticsearch Service) to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for API calls that used the access key to access an object that contained PII.
- D. Use Amazon Athena to query the CloudTrail logs in DOC-EXAMPLE-BUCKET2 for any API calls that used the access key to access an object that contained PII.
- E. Use AWS Identity and Access Management Access Analyzer to identify any API calls that used the access key to access objects that contained PII in DOC-EXAMPLE-BUCKET1.

Correct Answer: AD

QUESTION 2

A security engineer is designing an IAM policy for a script that will use the AWS CLI. The script currently assumes an IAM role that is attached to three AWS managed IAM policies: AmazonEC2FullAccess, AmazonDynamoDBFullAccess, and AmazonVPCFullAccess.

The security engineer needs to construct a least privilege IAM policy that will replace the AWS managed IAM policies that are attached to this role.

Which solution will meet these requirements in the MOST operationally efficient way?

- A. In AWS CloudTrail, create a trail for management events. Run the script with the existing AWS managed IAM policies. Use IAM Access Analyzer to generate a new IAM policy that is based on access activity in the trail. Replace the existing AWS managed IAM policies with the generated IAM policy for the role.
- B. Remove the existing AWS managed IAM policies from the role. Attach the IAM Access Analyzer Role Policy Generator to the role. Run the script. Return to IAM Access Analyzer and generate a least privilege IAM policy. Attach the new IAM policy to the role.



C. Create an account analyzer in IAM Access Analyzer. Create an archive rule that has a filter that checks whether the PrincipalArn value matches the ARN of the role. Run the script. Remove the existing AWS managed IAM policies from the role.

D. In AWS CloudTrail, create a trail for management events. Remove the existing AWS managed IAM policies from the role. Run the script. Find the authorization failure in the trail event that is associated with the script. Create a new IAM policy that includes the action and resource that caused the authorization failure. Repeat the process until the script succeeds. Attach the new IAM policy to the role.

Correct Answer: A

QUESTION 3

A recent security audit found that IAM CloudTrail logs are insufficiently protected from tampering and unauthorized access. Which actions must the Security Engineer take to address these audit findings? (Select THREE)

- A. Ensure CloudTrail log file validation is turned on
- B. Configure an S3 lifecycle rule to periodically archive CloudTrail logs into Glacier for long-term storage
- C. Use an S3 bucket with tight access controls that exists in a separate account
- D. Use Amazon Inspector to monitor the file integrity of CloudTrail log files.
- E. Request a certificate through ACM and use a generated certificate private key to encrypt CloudTrail log files
- F. Encrypt the CloudTrail log files with server-side encryption with IAM KMS-managed keys (SSE-KMS)

Correct Answer: ADE

QUESTION 4

A company has a web-based application using Amazon CloudFront and running on Amazon Elastic Container Service (Amazon ECS) behind an Application Load Balancer (ALB). The ALB is terminating TLS and balancing load across ECS service tasks. A security engineer needs to design a solution to ensure that application content is accessible only through CloudFront and that it is never accessible directly.

How should the security engineer build the MOST secure solution?

- A. Add an origin custom header. Set the viewer protocol policy to HTTP and HTTPS. Set the origin protocol policy to HTTPS only. Update the application to validate the CloudFront custom header.
- B. Add an origin custom header. Set the viewer protocol policy to HTTPS only. Set the origin protocol policy to match viewer. Update the application to validate the CloudFront custom header.
- C. Add an origin custom header. Set the viewer protocol policy to redirect HTTP to HTTPS. Set the origin protocol policy to HTTP only. Update the application to validate the CloudFront custom header.
- D. Add an origin custom header. Set the viewer protocol policy to redirect HTTP to HTTPS. Set the origin protocol policy to HTTPS only. Update the application to validate the CloudFront custom header.

Correct Answer: D



To ensure that application content is accessible only through CloudFront and not directly, the security engineer should do the following: Add an origin custom header. This is a header that CloudFront adds to the requests that it sends to the origin, but viewers cannot see or modify. Set the viewer protocol policy to redirect HTTP to HTTPS. This ensures that the viewers always use HTTPS when they access the website through CloudFront. Set the origin protocol policy to HTTPS only. This ensures that CloudFront always uses HTTPS when it connects to the origin. Update the application to validate the CloudFront custom header. This means that the application checks if the request has the custom header and only responds if it does. Otherwise, it denies or ignores the request. This prevents users from bypassing CloudFront and accessing the content directly on the origin.

QUESTION 5

A company's Security Engineer has been tasked with restricting a contractor's IAM account access to the company's Amazon EC2 console without providing access to any other AWS services. The contractor's IAM account must not be able to gain access to any other AWS service, even if the IAM account is assigned additional permissions based on IAM group membership.

What should the Security Engineer do to meet these requirements?

- A. Create an Inline IAM user policy that allows for Amazon EC2 access for the contractor's IAM user.
- B. Create an IAM permissions boundary policy that allows Amazon EC2 access. Associate the contractor's IAM account with the IAM permissions boundary policy.
- C. Create an IAM group with an attached policy that allows for Amazon EC2 access. Associate the contractor's IAM account with the IAM group.
- D. Create an IAM role that allows for EC2 and explicitly denies all other services. Instruct the contractor to always assume this role.

Correct Answer: B

[SCS-C02 VCE Dumps](#)

[SCS-C02 Practice Test](#)

[SCS-C02 Study Guide](#)