



SCS-C01^{Q&As}

AWS Certified Security - Specialty (SCS-C01)

Pass Amazon SCS-C01 Exam with 100% Guarantee

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

<https://www.passapply.com/aws-certified-security-specialty.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 is hosting a static website on Amazon S3. The company has configured an Amazon CloudFront distribution to serve the website contents. The company has associated an IAM WAF web ACL with the CloudFront distribution. The web ACL ensures that requests originate from the United States to address compliance restrictions.

THE company is worried that the S3 URL might still be accessible directly and that requests can bypass the CloudFront distribution.

Which combination of steps should the company take to remove direct access to the S3 URL? (Select TWO.)

- A. Select "Restrict Bucket Access" in the origin settings of the CloudFront distribution
- B. Create an origin access identity (OAI) for the S3 origin
- C. Update the S3 bucket policy to allow s3 GetObject with a condition that the IAM Referer key matches the secret value. Deny all other requests
- D. Configure the S3 bucket policy so that only the origin access identity (OAI) has read permission for objects in the bucket
- E. Add an origin custom header that has the name Referer to the CloudFront distribution. Give the header a secret value.

Correct Answer: AD

QUESTION 2

An organization policy states that all encryption keys must be automatically rotated every 12 months. Which AWS Key Management Service (KMS) key type should be used to meet this requirement?

- A. AWS managed Customer Master Key (CMK)
- B. Customer managed CMK with AWS generated key material
- C. Customer managed CMK with imported key material
- D. AWS managed data key

Correct Answer: B

QUESTION 3

A security team is implementing a centralized logging solution to meet requirements for auditing. The solution must be able to aggregate logs from Amazon CloudWatch and AWS CloudTrail to an account that is controlled by the security team. This approach must be usable across the entire organization in AWS Organizations.

Which solution meets these requirements in the MOST operationally efficient manner?

- A. In each AWS account, create an Amazon Kinesis Data Firehose delivery stream that has a destination of Amazon S3 in the security team's account. Create a subscription for each Amazon CloudWatch Logs log group in each AWS



account to the Kinesis Data Firehose delivery stream in the same account. For the organization, create a CloudTrail trail that has a destination of Amazon S3.

B. In the security team's account, create an Amazon Kinesis Data Firehose delivery stream that has a destination of Amazon S3 in the same account. Create a subscription for each Amazon CloudWatch Logs log group in each AWS account to the Kinesis Data Firehose delivery stream in the security team's account. For each AWS account, create a CloudTrail trail that has a destination of Amazon S3.

C. In each AWS account, create an Amazon Kinesis data stream that has a destination of Amazon S3 in the security team's account. Create a subscription for each Amazon CloudWatch Logs log group in each AWS account to the Kinesis data stream in the same account. For the organization, create a CloudTrail trail that has a destination of Amazon S3.

D. In the security team's account, create an Amazon Kinesis data stream that has a destination of Amazon S3 in the same account. Create a subscription for each Amazon CloudWatch Logs log group in each AWS account to the Kinesis data stream in the security team's account. For each AWS account, create a CloudTrail trail that has a destination of Amazon S3.

Correct Answer: A

QUESTION 4

You have an S3 bucket hosted in AWS. This is used to host promotional videos uploaded by yourself. You need to provide access to users for a limited duration of time. How can this be achieved? Please select:

- A. Use versioning and enable a timestamp for each version
- B. Use Pre-signed URL's
- C. Use IAM Roles with a timestamp to limit the access
- D. Use IAM policies with a timestamp to limit the access

Correct Answer: B

The AWS Documentation mentions the following All objects by default are private. Only the object owner has permission to access these objects. However, the object owner can optionally share objects with others by creating a pre-signed URL using their own security credentials, to grant time-limited permission to download the objects. Option A is invalid because this can be used to prevent accidental deletion of objects Option C is invalid because timestamps are not possible for Roles Option D is invalid because policies is not the right way to limit access based on time For more information on pre-signed URL's, please visit the URL:

<https://docs.aws.amazon.com/AmazonS3/latest/dev/ShareObjectPreSignedURL.html>

The correct answer is: Use Pre-signed URL's

QUESTION 5

An application is currently secured using network access control lists and security groups. Web servers are located in public subnets behind an Application Load Balancer (ALB); application servers are located in private subnets.

How can edge security be enhanced to safeguard the Amazon EC2 instances against attack? (Choose two.)

- A. Configure the application's EC2 instances to use NAT gateways for all inbound traffic.



- B. Move the web servers to private subnets without public IP addresses.
- C. Configure AWS WAF to provide DDoS attack protection for the ALB.
- D. Require all inbound network traffic to route through a bastion host in the private subnet.
- E. Require all inbound and outbound network traffic to route through an AWS Direct Connect connection.

Correct Answer: BC

[Latest SCS-C01 Dumps](#)

[SCS-C01 PDF Dumps](#)

[SCS-C01 Exam Questions](#)