# SCS-C02$^{\text{Q\&As}}$

AWS Certified Security - Specialty

**QUESTION 1**

A company stores images for a website in an Amazon S3 bucket. The company is using Amazon CloudFront to serve the images to end users. The company recently discovered that the images are being accessed from countries where the company does not have a distribution license.

Which actions should the company take to secure the images to limit their distribution? (Select TWO.)

A. Update the S3 bucket policy to restrict access to a CloudFront origin access identity (OAI).

B. Update the website DNS record to use an Amazon Route 53 geolocation record deny list of countries where the company lacks a license.

C. Add a CloudFront geo restriction deny list of countries where the company lacks a license.

D. Update the S3 bucket policy with a deny list of countries where the company lacks a license.

E. Enable the Restrict Viewer Access option in CloudFront to create a deny list of countries where the company lacks a license.

Correct Answer: AC

To secure the images to limit their distribution, the company should take the following actions:

Update the S3 bucket policy to restrict access to a CloudFront origin access identity (OAI). This allows the company to use a special CloudFront user that can access objects in their S3 bucket, and prevent anyone else from accessing them

directly.

Add a CloudFront geo restriction deny list of countries where the company lacks a license. This allows the company to use a feature that controls access to their content based on the geographic location of their viewers, and block requests

from countries where they do not have a distribution license.

**QUESTION 2**

A company wants to monitor the deletion of AWS Key Management Service (AWS KMS) customer managed keys. A security engineer needs to create an alarm that will notify the company before a KMS key is deleted. The security engineer has configured the integration of AWS CloudTrail with Amazon CloudWatch.

What should the security engineer do next to meet these requirements?

A. Specify the deletion time of the key material during KMS key creation. Create a custom AWS Config rule to assess the key\\'s scheduled deletion. Configure the rule to trigger upon a configuration change. Send a message to an Amazon Simple Notification Service (Amazon SNS) topic if the key is scheduled for deletion.

B. Create an Amazon EventBridge rule to detect KMS API calls of DeleteAlias. Create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) message to the company. Add the Lambda function as the target of the EventBridge rule.

C. Create an Amazon EventBridge rule to detect KMS API calls of DisableKey and ScheduleKeyDeletion. Create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) message to the company. Add the Lambda function as the target of the EventBridge rule.

D. Create an Amazon Simple Notification Service (Amazon SNS) policy to detect KMS API calls of RevokeGrant and ScheduleKeyDeletion. Create an AWS Lambda function to generate the alarm and send the notification to the company. Add the Lambda function as the target of the SNS policy.

Correct Answer: C

The AWS documentation states that you can create an Amazon EventBridge rule to detect KMS API calls of DisableKey and ScheduleKeyDeletion. You can then create an AWS Lambda function to send an Amazon Simple Notification Service (Amazon SNS) message to the company. You can add the Lambda function as the target of the EventBridge rule. This method will meet the requirements. References: AWS KMS Developer Guide

## QUESTION 3

Which of the following are valid configurations for using SSL certificates with Amazon CloudFront? (Select THREE )

A. Default AWS Certificate Manager certificate

B. Custom SSL certificate stored in AWS KMS

C. Default CloudFront certificate

D. Custom SSL certificate stored in AWS Certificate Manager

E. Default SSL certificate stored in AWS Secrets Manager

F. Custom SSL certificate stored in AWS IAM

Correct Answer: ABC

The key length for an RSA certificate that you use with CloudFront is 2048 bits, even though ACM supports larger keys. If you use an imported certificate with CloudFront, your key length must be 1024 or 2048 bits and cannot exceed 2048 bits. You must import the certificate in the US East (N. Virginia) Region. You must have permission to use and import the SSL/TLS certificate https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/cnames-and-httpsrequirements.html

## QUESTION 4

A company deployed Amazon GuardDuty In the us-east-1 Region. The company wants all DNS logs that relate to the company\\'s Amazon EC2 instances to be inspected. What should a security engineer do to ensure that the EC2 instances are logged?

A. Use IPv6 addresses that are configured for hostnames.

B. Configure external DNS resolvers as internal resolvers that are visible only to IAM.

C. Use IAM DNS resolvers for all EC2 instances.

D. Configure a third-party DNS resolver with logging for all EC2 instances.

Correct Answer: C

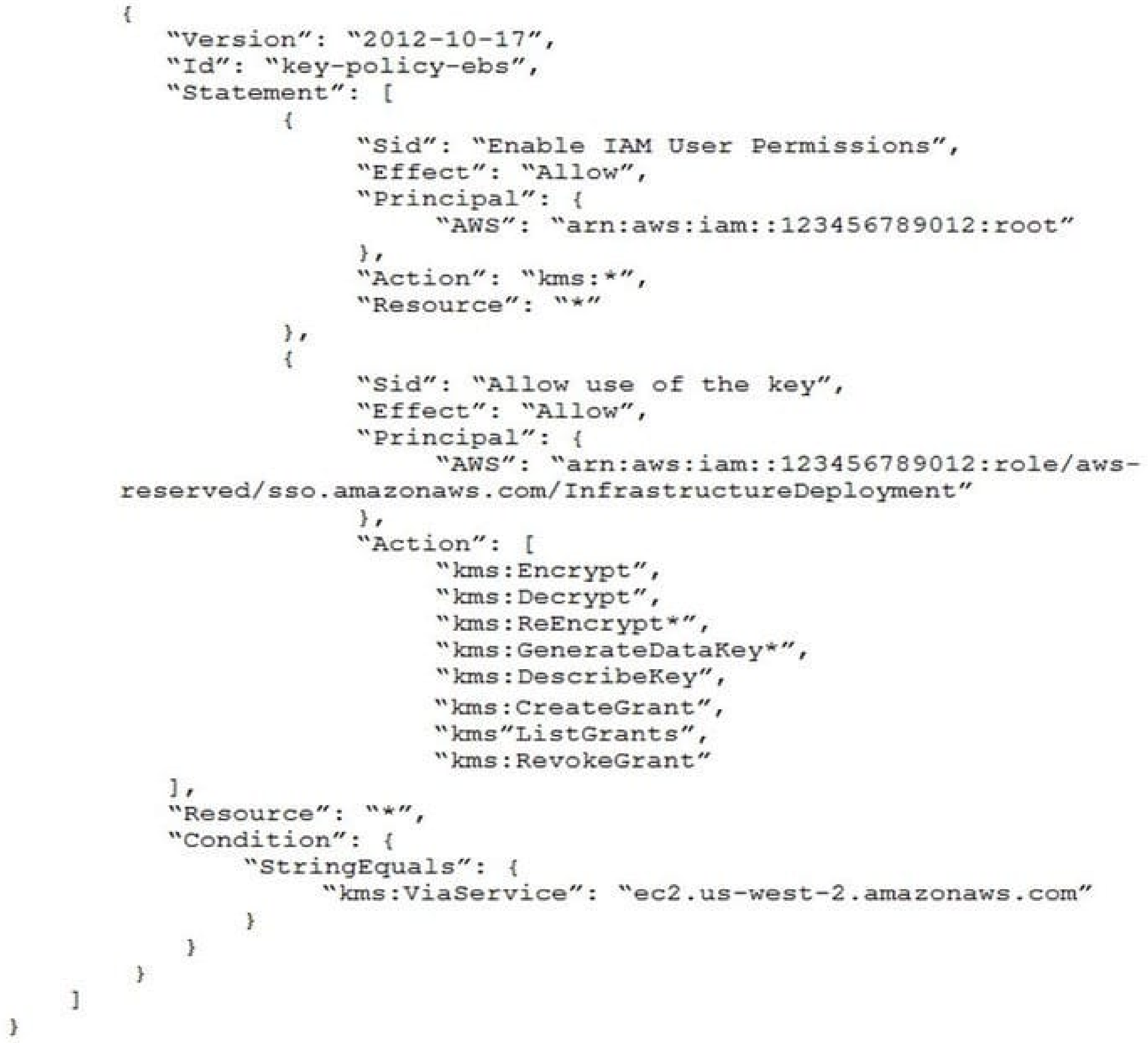
To ensure that the EC2 instances are logged, the security engineer should do the following:

Use AWS DNS resolvers for all EC2 instances. This allows the security engineer to use Amazon-provided DNS servers that resolve public DNS hostnames to private IP addresses within their VPC, and that log DNS queries in Amazon

CloudWatch Logs.

**QUESTION 5**

A company wants to establish separate IAM Key Management Service (IAM KMS) keys to use for different IAM services. The company\\'s security engineer created the following key policy lo allow the infrastructure deployment team to create encrypted Amazon Elastic Block Store (Amazon EBS) volumes by assuming the InfrastructureDeployment IAM role:



```
      {
         “Version”: “2012-10-17”,
         “Id”: “key-policy-ebs”,
         “Statement”: [
                {
                     “Sid”: “Enable IAM User Permissions”,
                     “Effect”: “Allow”,
                     “Principal”: {
                          “AWS”: “arn:aws:iam::123456789012:root”
                     },
                     “Action”: “kms:*”,
                     “Resource”: “*”
                },
                {
                     “Sid”: “Allow use of the key”,
                     “Effect”: “Allow”,
                     “Principal”: {
                          “AWS”: “arn:aws:iam::123456789012:role/aws-
      reserved/sso.amazonaws.com/InfrastructureDeployment”
                     },
                     “Action”: [
                          “kms:Encrypt”,
                          “kms:Decrypt”,
                          “kms:ReEncrypt*”,
                          “kms:GenerateDataKey*”,
                          “kms:DescribeKey”,
                          “kms:CreateGrant”,
                          “kms”ListGrants”,
                          “kms:RevokeGrant”
         ],
         “Resource”: “*”,
         “Condition”: {
              “StringEquals”: {
                   “kms:ViaService”: “ec2.us-west-2.amazonaws.com”
              }
         }
      }
   ]
}
```

The security engineer recently discovered that IAM roles other than the InfrastructureDeployment role used this key (or 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 Dlock 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 .amazonIAM com.

D. In the policy document, add a new statement block that grants the kms:Disable\\' permission to the security engineer\\'s IAM role.

Correct Answer: C

To resolve the issues, the security engineer should make the following change to the policy:

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. This allows the security engineer to restrict the use of the key to only EC2

service in the us-east-1 region, and prevent other services from using the key.

SCS-C02 Study Guide SCS-C02 Exam Questions SCS-C02 Braindumps