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.pass4itsure.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 guideline that mandates the encryption of all Amazon S3 bucket data in transit. A security engineer must implement an S3 bucket policy that denies any S3 operations if data is not encrypted.

A.
```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowSSLRequestOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
          "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
          "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        ],
        "Condition": {
          "Bool": {
              "aws:SecureTransport": "true"
          }
        },
        "Principal": "*"
    }]
}
```

B.
```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowSSLRequestOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
          "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
          "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
        ],
        "Condition": {
          "Bool": {
              "aws:SecureTransport": "false"
          }
        },
        "Principal": "*"
    }]
}
```

Which S3 bucket policy will meet this requirement?

C.
```
{
    "Version": "2012-10-17",
    "Statement": [{
                "Sid": "AllowSSLRequestOnly",
                "Action": "s3:*",
                "Effect": "Deny",
                "Resource": [
                  "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                  "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
                ],
                "Condition": {
                  "StringNotEquals": {
                      "s3:x-amz-server-side-encryption": "AES256"
                  }
                },
                "Principal": "*"
    }]
}
```

D.
```
{
    "Version": "2012-10-17",
    "Statement": [{
                "Sid": "AllowSSLRequestOnly",
                "Action": "s3:*",
                "Effect": "Deny",
                "Resource": [
                  "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
                  "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
                ],
                "Condition": {
                  "StringNotEquals": {
                      "s3:x-amz-server-side-encryption": true
                  }
                },
                "Principal": "*"
    }]
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: B

https://aws.amazon.com/blogs/security/how-to-use-bucket-policies-and-apply-defense-in-depth-to-help-secure-your-amazon-s3-data/

QUESTION 2

A Security Engineer is troubleshooting an issue with a company\\'s custom logging application. The application logs are written to an Amazon S3 bucket with event notifications enabled to send events lo an Amazon SNS topic. All logs are encrypted at rest using an IAM KMS CMK. The SNS topic is subscribed to an encrypted Amazon SQS queue. The logging application polls the queue for new messages that contain metadata about the S3 object. The application then reads the content of the object from the S3 bucket for indexing.

The Logging team reported that Amazon CloudWatch metrics for the number of messages sent or received is showing zero. No togs are being received.

What should the Security Engineer do to troubleshoot this issue?

A. Add the following statement to the IAM managed CMKs:

```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": ["sns.amazonaws.com", "sqs.amazonaws.com", "s3.amazonaws.com"]
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

B. Add the following statement to the CMK key policy:

```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": "sns.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

C. Add the following statement to the CMK key policy:

```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": "sqs.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

D. Add the following statement to the CMK key policy:

```
{
    "Sid": "Allow Amazon SNS to use this key",
    "Effect": "Allow",
    "Principal": {
        "Service": "s3.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*"
}
```

A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: D

QUESTION 3

A security engineer configures Amazon S3 Cross-Region Replication (CRR) for all objects that are in an S3 bucket in the us-east-1. Region Some objects in this S3 bucket use server-side encryption with AWS KMS keys (SSE-KMS) for encryption at test. The security engineer creates a destination S3 bucket in the us-west-2 Region. The destination S3 bucket is in the same AWS account as the source S3 bucket.

The security engineer also creates a customer managed key in us-west-2 to encrypt objects at rest in the destination S3 bucket. The replication configuration is set to use the key in us-west-2 to encrypt objects in the destination S3 bucket. The security engineer has provided the S3 replication configuration with an IAM role to perform the replication in Amazon S3.

After a day, the security engineer notices that no encrypted objects from the source S3 bucket are replicated to the destination S3 bucket. However, all the unencrypted objects are replicated.

Which combination of steps should the security engineer take to remediate this issue? (Select THREE.)

A. Change the replication configuration to use the key in us-east-1 to encrypt the objects that are in the destination S3 bucket.

B. Grant the IAM role the kms. Encrypt permission for the key in us-east-1 that encrypts source objects.

C. Grant the IAM role the s3 GetObjectVersionForReplication permission for objects that are in the source S3 bucket.

D. Grant the IAM role the kms. Decrypt permission for the key in us-east-1 that encrypts source objects.

E. Change the key policy of the key in us-east-1 to grant the kms. Decrypt permission to the security engineer\\'s IAM account.

F. Grant the IAM role the kms Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket.

Correct Answer: BF

To enable S3 Cross-Region Replication (CRR) for objects that are encrypted with SSE-KMS, the following steps are required:

Grant the IAM role the kms.Decrypt permission for the key in us-east-1 that encrypts source objects. This will allow the IAM role to decrypt the source objects before replicating them to the destination bucket. The kms.Decrypt permission must

be granted in the key policy of the source KMS key or in an IAM policy attached to the IAM role.

Grant the IAM role the kms.Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket. This will allow the IAM role to encrypt the replica objects with the destination KMS key before storing them in

the destination bucket. The kms.Encrypt permission must be granted in the key policy of the destination KMS key or in an IAM policy attached to the IAM role. This solution will remediate the issue of encrypted objects not being replicated to

the destination bucket.

The other options are incorrect because they either do not grant the necessary permissions for CRR (A, C, D), or do not use a valid encryption method for CRR (E).

Verified References:

https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html

QUESTION 4

A security engineer is configuring a new website that is named example.com. The security engineer wants to secure communications with the website by requiring users to connect to example.com through HTTPS.

Which of the following is a valid option for storing SSL/TLS certificates?

A. Custom SSL certificate that is stored in AWS Key Management Service (AWS KMS)

B. Default SSL certificate that is stored in Amazon CloudFront.

C. Custom SSL certificate that is stored in AWS Certificate Manager (ACM)

D. Default SSL certificate that is stored in Amazon S3

Correct Answer: C

QUESTION 5

A company uses AWS Organizations. The company has teams that use an AWS CloudHSM hardware security module (HSM) that is hosted in a central AWS account. One of the teams creates its own new dedicated AWS account and wants to use the HSM that is hosted in the central account.

How should a security engineer share the HSM that is hosted in the central account with the new dedicated account?

A. Use AWS Resource Access Manager (AWS RAM) to share the VPC subnet ID of the HSM that is hosted in the central account with the new dedicated account. Configure the CloudHSM security group to accept inbound traffic from the private IP addresses of client instances in the new dedicated account.

B. Use AWS Identity and Access Management (IAM) to create a cross-account rote to access the CloudHSM cluster that is in the central account Create a new IAM user in the new dedicated account Assign the cross-account rote to the new IAM user.

C. Use AWS 1AM Identity Center (AWS Single Sign-On) to create an AWS Security Token Service (AWS STS) token to authenticate from the new dedicated account to the central account. Use the cross-account permissions that are assigned to the STS token to invoke an operation on the HSM in the central account.

D. Use AWS Resource Access Manager (AWS RAM) to share the ID of the HSM that is hosted in the central account with the new dedicated account. Configure the CloudHSM security group to accept inbound traffic from the private IP addresses of client instances in the new dedicated account.

Correct Answer: A

https://aws.amazon.com/premiumsupport/knowledge-center/cloudhsm-share-clusters/#:~:text=In%20the%20navigation%20pane%2C%20in,subnet%20ID%20for%20your%20CloudHSM.