SCS-C01$^{\text{Q\&As}}$

AWS Certified Security - Specialty (SCS-C01)

QUESTION 1

An organization has a multi-petabyte workload that it is moving to Amazon S3, but the CISO is concerned about cryptographic wear-out and the blast radius if a key is compromised.

How can the CISO be assured that AWS KMS and Amazon S3 are addressing the concerns? (Choose two.)

A. There is no API operation to retrieve an S3 object in its encrypted form.

B. Encryption of S3 objects is performed within the secure boundary of the KMS service.

C. S3 uses KMS to generate a unique data key for each individual object.

D. Using a single master key to encrypt all data includes having a single place to perform audits and usage validation.

E. The KMS encryption envelope digitally signs the master key during encryption to prevent cryptographic wear-out

Correct Answer: AC

A. Correct. When SSE-KMS is enabled, S3 won\\'t return an object if the user doesn\\'t have permissions to use the CMK to decrypt. If the user does have permissions, they\\'ll get clear-text data back, not encrypted. Limits cryptanalysis necessary for "key wear-out".

B. Incorrect since S3 doesn\\'t encrypt/decrypt objects within KMS - only the data-encryption keys. The objects are encrypted/decrypted in S3.

C. Correct - limits blast radius.

D. Incorrect the data is larger than the very small 4KB limit for data-encryption using a CMK directly. S3 doesn\\'t do this anyway - it creates DEKs for each object (which is why C is applicable for blast-radius).

E. Cryptographic wear-out is a loose term that describes a condition where enough data has been encrypted by a key to make cryptanalyis somewhat feasible. Signing a master key would have no effect.

QUESTION 2

A Development team has built an experimental environment to test a simple stale web application It has built an isolated VPC with a private and a public subnet. The public subnet holds only an Application Load Balancer a NAT gateway, and an internet gateway. The private subnet holds ail of the Amazon EC2 instances There are 3 different types of servers Each server type has its own Security Group that limits access lo only required connectivity. The Security Groups nave both inbound and outbound rules applied Each subnet has both inbound and outbound network ACls applied to limit access to only required connectivity

Which of the following should the team check if a server cannot establish an outbound connection to the internet? (Select THREE.)

A. The route tables and the outbound rules on the appropriate private subnet security group

B. The outbound network ACL rules on the private subnet and the Inbound network ACL rules on the public subnet

C. The outbound network ACL rules on the private subnet and both the inbound and outbound rules on the public subnet

D. The rules on any host-based firewall that may be applied on the Amazon EC2 instances

E. The Security Group applied to the Application Load Balancer and NAT gateway

F. That the 0.0.0./0 route in the private subnet route table points to the internet gateway in the public subnet

Correct Answer: CEF

QUESTION 3

A company has a security team that manages its AWS Key Management Service (AWS KMS) CMKs. Members of the security team must be the only ones to administer the CMKs. The company\\'s application team has a software process that needs temporary access to the CMKS occasionally. The security team must provide the application team\\'s software process access to the CMKs.

Which solution meets these requirements with the LEAST overhead?

A. Export the CMK 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 CMKs by adding the application team as principals. Revert this change when the application team no longer needs access.

C. Create a key grant to allow the application team to use the CMKs. Revoke the grant when the application team no longer needs access.

D. Create a new CMK by generating key material on premises. Import the key material to AWS KMS whenever the application team needs access. Grant the application team permissions to use the CMK.

Correct Answer: C

QUESTION 4

A company will store sensitive documents in three Amazon S3 buckets based on a data classification scheme of "Sensitive," "Confidential," and "Restricted." The security solution must meet all of the following requirements:

1.

Each object must be encrypted using a unique key. Items that are stored in the "Restricted" bucket require two-factor authentication for decryption.

2.

AWS KMS must automatically rotate encryption keys annually. Which of the following meets these requirements?

A. Create a Customer Master Key (CMK) for each data classification type, and enable the rotation of it annually. For the "Restricted" CMK, define the MFA policy within the key policy. Use S3 SSE-KMS to encrypt the objects.

B. Create a CMK grant for each data classification type with EnableKeyRotation and MultiFactorAuthPresent set to true. S3 can then use the grants to encrypt each object with a unique CMK.

C. Create a CMK for each data classification type, and within the CMK policy, enable rotation of it annually, and define the MFA policy. S3 can then create DEK grants to uniquely encrypt each object within the S3 bucket.

D. Create a CMK with unique imported key material for each data classification type, and rotate them annually. For the "Restricted" key material, define the MFA policy in the key policy. Use S3 SSE-KMS to encrypt the objects.

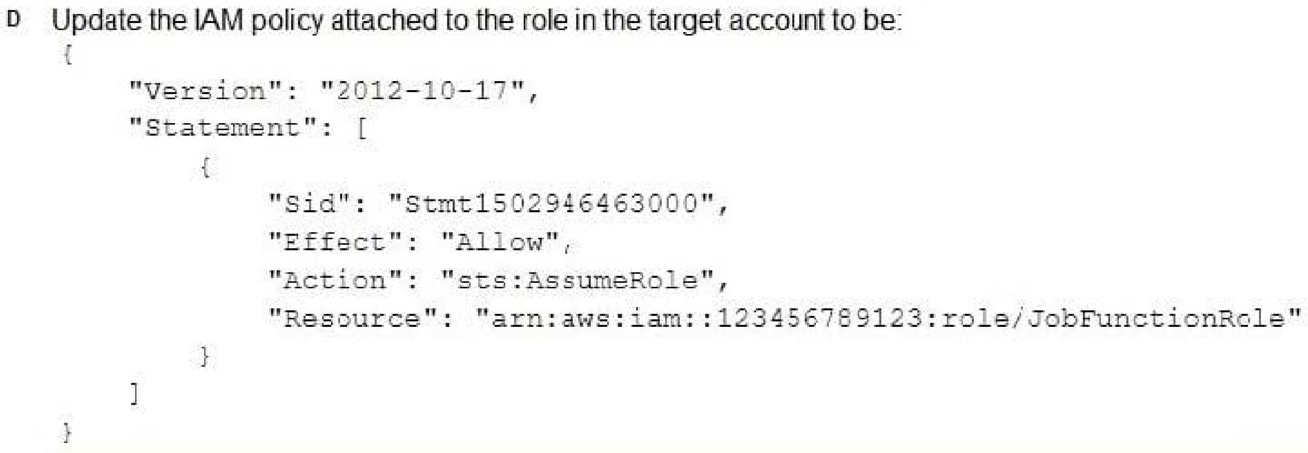
Correct Answer: A

CMKs that are not eligible for automatic key rotation, including asymmetric CMKs, CMKs in custom key stores, and CMKs with imported key material.

QUESTION 5

A security engineer is defining the controls required to protect the AWS account root user credentials in an AWS Organizations hierarchy. The controls should also limit the impact in case these credentials have been compromised.

Which combination of controls should the security engineer propose? (Choose three.)



D Update the IAM policy attached to the role in the target account to be:

```
{
     "Version": "2012-10-17",
     "Statement": [
          {
               "Sid": "Stmt1502946463000",
               "Effect": "Allow",
               "Action": "sts:AssumeRole",
               "Resource": "arn:aws:iam::123456789123:role/JobFunctionRole"
          }
     ]
}
```

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

F. Option F

Correct Answer: ADF