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.leads4pass.com/scs-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Amazon Official Exam Center

QUESTION 1

A company needs its Amazon Elastic Block Store (Amazon EBS) volumes to be encrypted at all times. During a security incident. EBS snapshots of suspicious instances are shared to a forensics account for analysis A security engineer attempting to share a suspicious EBS snapshot to the forensics account receives the following error

"Unable to share snapshot: An error occurred (OperationNotPermitted) when calling the ModifySnapshotAttribute operation: Encrypted snapshots with EBS default key cannot be shared.

Which combination of steps should the security engineer take in the incident account to complete the sharing operation? (Select THREE)

A. Create a customer managed CMK Copy the EBS snapshot encrypting the destination snapshot using the new CMK.

B. Allow forensics accounting principals to use the CMK by modifying its policy.

C. Create an Amazon EC2 instance. Attach the encrypted and suspicious EBS volume. Copy data from the suspicious volume to an unencrypted volume. Snapshot the unencrypted volume

D. Copy the EBS snapshot to the new decrypted snapshot

E. Restore a volume from the suspicious EBS snapshot. Create an unencrypted EBS volume of the same size.

F. Share the target EBS snapshot with the forensics account.

Correct Answer: ABF

QUESTION 2

A company plans to move most of its IT infrastructure to IAM. They want to leverage their existing on-premises Active Directory as an identity provider for IAM.

Which combination of steps should a Security Engineer take to federate the company\\'s on- premises Active Directory with IAM? (Choose two.)

A. Create IAM roles with permissions corresponding to each Active Directory group.

B. Create IAM groups with permissions corresponding to each Active Directory group.

C. Configure Amazon Cloud Directory to support a SAML provider.

D. Configure Active Directory to add relying party trust between Active Directory and IAM.

E. Configure Amazon Cognito to add relying party trust between Active Directory and IAM.

Correct Answer: AD

https://IAM.amazon.com/blogs/security/how-to-establish-federated-access-to-your-IAM- resources-by-using-active-directory-user-attributes/

QUESTION 3

A company uses AWS Organizations to manage several AWs accounts. The company processes a large volume of sensitive data. The company uses a serverless approach to microservices. The company stores all the data in either Amazon S3 or Amazon DynamoDB. The company reads the data by using either AWS lambda functions or container-based services that the company hosts on Amazon Elastic Kubernetes Service (Amazon EKS) on AWS Fargate.

The company must implement a solution to encrypt all the data at rest and enforce least privilege data access controls. The company creates an AWS Key Management Service (AWS KMS) customer managed key.

What should the company do next to meet these requirements?

A. Create a key policy that allows the kms:Decrypt action only for Amazon S3 and DynamoDB. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.

B. Create an 1AM policy that denies the kms:Decrypt action for the key. Create a Lambda function than runs on a schedule to attach the policy to any new roles. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.

C. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EKS. Create an SCP that denies the creation of S3 buckets and DynamoDB tables that are not encrypted with the key.

D. Create a key policy that allows the kms:Decrypt action only for Amazon S3, DynamoDB, Lambda, and Amazon EKS. Create an AWS Config rule to send alerts for resources that are not encrypted with the key.

Correct Answer: C

QUESTION 4

An IT department currently has a Java web application deployed on Apache Tomcat running on Amazon EC2 instances. All traffic to the EC2 instances is sent through an internet-facing Application Load Balancer (ALB) The Security team has noticed during the past two days thousands of unusual read requests coming from hundreds of IP addresses. This is causing the Tomcat server to run out of threads and reject new connections

Which the SIMPLEST change that would address this server issue?

A. Create an Amazon CloudFront distribution and configure the ALB as the origin

B. Block the malicious IPs with a network access list (NACL).

C. Create an IAM Web Application Firewall (WAF). and attach it to the ALB

D. Map the application domain name to use Route 53

Correct Answer: A

QUESTION 5

A company\\'s Security Engineer is copying all application logs to centralized Amazon S3 buckets. Currently, each of the company\\'s applications is in its own IAM account, and logs are pushed into S3 buckets associated with each account. The Engineer will deploy an IAM Lambda function into each account that copies the relevant log files to the centralized S3 bucket.

The Security Engineer is unable to access the log files in the centralized S3 bucket. The Engineer\\'s IAM user policy from the centralized account looks like this:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": "s3:Put*",
            "Resource":"arn:aws:s3:::centralizedbucket/*",
            "Effect": "Deny"
        },
        {
            "Action": ["s3:Get*","s3:List*"],
            "Resource": [
                "arn:aws:s3:::centralizedbucket/*",
                "arn:aws:s3:::centralizedbucket/"
            ],
            "Effect": "Allow"
        }
    ]
}
```

The centralized S3 bucket policy looks like this:

```
{
    "Version": "2012-10-17",    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:role/LogCopier",
                    "arn:aws:iam::444455556666:role/LogCopier"
                ]
            },
            "Action": ["s3:PutObject","s3:PutObjectAcl"],
            "Resource": "arn:aws:s3:::centralizedbucket/*"
        }
    ]
}
```

Why is the Security Engineer unable to access the log files?

A. The S3 bucket policy does not explicitly allow the Security Engineer access to the objects in the bucket.

B. The object ACLs are not being updated to allow the users within the centralized account to access the objects

C. The Security Engineers IAM policy does not grant permissions to read objects in the S3 bucket

D. The s3:PutObject and s3:PutObjectAcl permissions should be applied at the S3 bucket level

Correct Answer: C

QUESTION 6

One of the EC2 Instances in your company has been compromised. What steps would you take to ensure that you could apply digital forensics on the Instance? Select 2 answers from the options given below

A. Remove the role applied to the Ec2 Instance

B. Create a separate forensic instance

C. Ensure that the security groups only allow communication to this forensic instance

D. Terminate the instance

Correct Answer: BC

Option A is invalid because removing the role will not help completely in such a situation Option D is invalid because terminating the instance means that you cannot conduct forensic analysis on the instance One way to isolate an affected EC2 instance for investigation is to place it in a Security Group that only the forensic investigators can access. Close all ports except to receive inbound SSH or RDP traffic from one single IP address from which the investigators can safely examine the instance. For more information on security scenarios for your EC2 Instance, please refer to below URL: https://d1.IAMstatic.com/Marketplace/scenarios/security/SEC 11 TSB Final.pd1 The correct answers are: Create a separate forensic instance. Ensure that the security groups only allow communication to this forensic instance Submit your Feedback/Queries to our Experts

---

QUESTION 7

A company plans to migrate a sensitive dataset to Amazon S3. A Security Engineer must ensure that the data is encrypted at rest. The encryption solution must enable the company to generate its own keys without needing to manage key storage or the encryption process.

What should the Security Engineer use to accomplish this?

A. Server-side encryption with Amazon S3-managed keys (SSE-S3)

B. Server-side encryption with IAM KMS-managed keys (SSE-KMS)

C. Server-side encryption with customer-provided keys (SSE-C)

D. Client-side encryption with an IAM KMS-managed CMK

Correct Answer: B

Reference https://IAM.amazon.com/s3/faqs/

QUESTION 8

A Security Engineer is setting up a new IAM account. The Engineer has been asked to continuously monitor the company\\'s IAM account using automated compliance checks based on IAM best practices and Center for Internet Security (CIS) IAM Foundations Benchmarks

How can the Security Engineer accomplish this using IAM services?

A. Enable IAM Config and set it to record all resources in all Regions and global resources. Then enable IAM Security

Hub and confirm that the CIS IAM Foundations compliance standard is enabled

B. Enable Amazon Inspector and configure it to scan all Regions for the CIS IAM Foundations Benchmarks. Then enable IAM Security Hub and configure it to ingest the Amazon Inspector findings

C. Enable Amazon Inspector and configure it to scan all Regions for the CIS IAM Foundations Benchmarks. Then enable IAM Shield in all Regions to protect the account from DDoS attacks.

D. Enable IAM Config and set it to record all resources in all Regions and global resources Then enable Amazon Inspector and configure it to enforce CIS IAM Foundations Benchmarks using IAM Config rules.

Correct Answer: A

https://docs.IAM.amazon.com/securityhub/latest/userguide/securityhub- standards-cis-config-resources.html

QUESTION 9

A recent security audit identified that a company\\'s application team injects database credentials into the environment variables of an IAM Fargate task. The company\\'s security policy mandates that all sensitive data be encrypted at rest and in transit.

When combination of actions should the security team take to make the application compliant within the security policy? (Select THREE)

A. Store the credentials securely in a file in an Amazon S3 bucket with restricted access to the application team IAM role Ask the application team to read the credentials from the S3 object instead

B. Create an IAM Secrets Manager secret and specify the key/value pairs to be stored in this secret

C. Modify the application to pull credentials from the IAM Secrets Manager secret instead of the environment variables.

D. Add the following statement to the container instance IAM role policy

```
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameters",
        "secretsmanager:GetSecretValue",
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
        "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
    ]
}
```

E. Add the following statement to the execution role policy.

```
{
    "Effect": "Allow",
    "Action": [
        "ssm:GetParameters",
        "secretsmanager:GetSecretValue",
        "kms:Decrypt"
    ],
    "Resource": [
        "arn:aws:secretsmanager:<region>:<aws_account_id>:secret:secret_name",
        "arn:aws:kms:<region>:<aws_account_id>:key/key_id"
    ]
}
```

F. Log in to the IAM Fargate instance, create a script to read the secret value from IAM Secret Manager, and inject the environment variables. Ask the application team to redeploy the application.

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

F. Option F

Correct Answer: BEF

QUESTION 10

A security engineer needs to create an IAM Key Management Service