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.pass4itsure.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

QUESTION 1

A company has a set of resources defined in AWS. It is mandated that all API calls to the resources be monitored. Also all API calls must be stored for lookup purposes. Any log data greater than 6 months must be archived. Which of the following meets these requirements? Choose 2 answers from the options given below. Each answer forms part of the solution.

Please select:

A. Enable CloudTrail logging in all accounts into S3 buckets

B. Enable CloudTrail logging in all accounts into Amazon Glacier

C. Ensure a lifecycle policy is defined on the S3 bucket to move the data to EBS volumes after 6 months.

D. Ensure a lifecycle policy is defined on the S3 bucket to move the data to Amazon Glacier after 6 months.

Correct Answer: AD

Cloudtrail publishes the trail of API logs to an S3 bucket

Option B is invalid because you cannot put the logs into Glacier from CloudTrail

Option C is invalid because lifecycle policies cannot be used to move data to EBS volumes

For more information on Cloudtrail logging, please visit the below URL:

https://docs.aws.amazon.com/awscloudtrail/latest/usereuide/cloudtrail-find-log-files.htmll

You can then use Lifecycle policies to transfer data to Amazon Glacier after 6 months For more information on S3 lifecycle policies, please visit the below URL:

https://docs.aws.amazon.com/AmazonS3/latest/dev/object-lifecycle-mgmt.html

The correct answers are: Enable CloudTrail logging in all accounts into S3 buckets. Ensure a lifecycle policy is defined on the bucket to move the data to Amazon Glacier after 6 months.

QUESTION 2

An application has been built with Amazon EC2 instances that retrieve messages from Amazon SQS. Recently, IAM changes were made and the instances can no longer retrieve messages.

What actions should be taken to troubleshoot the issue while maintaining least privilege. (Select two.)

A. Configure and assign an MFA device to the role used by the instances.

B. Verify that the SQS resource policy does not explicitly deny access to the role used by the instances.

C. Verify that the access key attached to the role used by the instances is active.

D. Attach the AmazonSQSFullAccess managed policy to the role used by the instances.

E. Verify that the role attached to the instances contains policies that allow access to the queue.

Correct Answer: BE

QUESTION 3

You are planning on using the AWS KMS service for managing keys for your application. For which of the following can the KMS CMK keys be used for encrypting? Choose 2 answers from the options given below

Please select:

A. Image Objects

B. Large files

C. Password

D. RSA Keys

Correct Answer: CD

The CMK keys themselves can only be used for encrypting data that is maximum 4KB in size. Hence it can be used for encryptii information such as passwords and RSA keys. Option A and B are invalid because the actual CMK key can only be used to encrypt small amounts of data and not large amoui of data. You have to generate the data key from the CMK key in order to encrypt high amounts of data For more information on the concepts for KMS, please visit the following URL: https://docs.aws.amazon.com/kms/latest/developereuide/concepts.htmll The correct answers are: Password, RSA Keys

QUESTION 4

In order to encrypt data in transit for a connection to an AWS RDS instance, which of the following would you implement

Please select:

A. Transparent data encryption

B. SSL from your application

C. Data keys from AWS KMS

D. Data Keys from CloudHSM

Correct Answer: B

This is mentioned in the AWS Documentation You can use SSL from your application to encrypt a connection to a DB instance running MySQL MariaDB, Amazon Aurora, SQL Server, Oracle, or PostgreSQL.

Option A is incorrect since Transparent data encryption is used for data at rest and not in transit

Options C and D are incorrect since keys can be used for encryption of data at rest For more information on working with RDS and SSL, please refer to below URL:

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/UsingWithRDS.SSL.html The correct answer is: SSL from your application

QUESTION 5

A Security Engineer must design a solution that enables the Incident Response team to audit for changes to a user\\'s IAM permissions in the case of a security incident. How can this be accomplished?

A. Use AWS Config to review the IAM policy assigned to users before and after the incident.

B. Run the GenerateCredentialReport via the AWS CLI, and copy the output to Amazon S3 daily for auditing purposes.

C. Copy AWS CloudFormation templates to S3, and audit for changes from the template.

D. Use Amazon EC2 Systems Manager to deploy images, and review AWS CloudTrail logs for changes.

Correct Answer: A

https://aws.amazon.com/blogs/security/how-to-record-and-govern-your-iam-resource-configurations-using-aws-config/