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.leads4pass.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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A company has two AWS accounts: Account A and Account B. Account A has an IAM role that IAM users in Account B assume when they need to upload sensitive documents to Amazon S3 buckets in Account A.

A new requirement mandates that users can assume the role only if they are authenticated with multi-factor authentication (MFA). A security engineer must recommend a solution that meets this requirement with minimum risk and effort. Which solution should the security engineer recommend?

A. Add an aws:MultiFactorAuthPresent condition to the role\\'s permissions policy.

B. Add an aws:MultiFactorAuthPresent condition to the role\\'s trust policy.

C. Add an aws:MultiFactorAuthPresent condition to the session policy.

D. Add an aws:MultiFactorAuthPresent condition to the S3 bucket policies.

Correct Answer: D

QUESTION 2

You want to launch an EC2 Instance with your own key pair in AWS. How can you achieve this? Choose 3 answers from the options given below.

Please select:

A. Use a third party tool to create the Key pair

B. Create a new key pair using the AWS CLI

C. Import the public key into EC2

D. Import the private key into EC2

Correct Answer: ABC

This is given in the AWS Documentation Creating a Key Pair You can use Amazon EC2 to create your key pair. For more information, see Creating a Key Pair Using Amazon EC2. Alternatively, you could use a third-party tool and then import the public key to Amazon EC2. For more information, see Importing Your Own Public Key to Amazon EC2. Option B is Correct, because you can use the AWS CLI to create a new key pair 1 https://docs.aws.amazon.com/cli/latest/userguide/ cli-ec2-keypairs.html Option D is invalid because the public key needs to be stored in the EC2 Instance For more information on EC2 Key pairs, please visit the below URL:

* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs

The correct answers are: Use a third party tool to create the Key pair. Create a new key pair using the AWS CLI, Import the public key into EC2

QUESTION 3

A company\\'s security engineer receives an abuse notification from AWS. The notification indicates that someone is

hosting malware from the company\\'s AWS account. After investigation, the security engineer finds a new Amazon S3 bucket that an IAM user created without authorization.

Which combination of steps should the security engineer take to MINIMIZE the consequences of this compromise? (Choose three.)

A. Encrypt all AWS CloudTrail logs.

B. Turn on Amazon GuardDuty.

C. Change the password for all IAM users.

D. Rotate or delete all AWS access keys.

E. Take snapshots of all Amazon Elastic Block Store (Amazon EBS) volumes.

F. Delete any resources that are unrecognized or unauthorized.

Correct Answer: BDE

QUESTION 4

A company hosts a web-based application that captures and stores sensitive data in an Amazon DynamoDB table. A security audit reveals that the application does not provide end-to-end data protection or the ability to detect unauthorized data changes The software engineering team needs to make changes that will address the audit findings.

Which set of steps should the software engineering team take?

A. Use an AWS Key Management Service (AWS KMS) CMK. Encrypt the data at rest.

B. Use AWS Certificate Manager (ACM) Private Certificate Authority Encrypt the data in transit.

C. Use a DynamoDB encryption client. Use client-side encryption and sign the table items

D. Use the AWS Encryption SDK. Use client-side encryption and sign the table items.

Correct Answer: A

QUESTION 5

Your company has a set of EC2 Instances defined in AWS. They need to ensure that all traffic packets are monitored and inspected for any security threats. How can this be achieved? Choose 2 answers from the options given below

Please select:

A. Use a host based intrusion detection system

B. Use a third party firewall installed on a central EC2 instance

C. Use VPC Flow logs

D. Use Network Access control lists logging

Correct Answer: AB

If you want to inspect the packets themselves, then you need to use custom based software A diagram representation of this is given in the AWS Security best practices

```
{
    "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/*"
        }
    ]
}
```

Option C is invalid because VPC Flow logs cannot conduct packet inspection. For more information on AWS Security best practices, please refer to below URL: The correct answers are: Use a host based intrusion detection system. Use a third party firewall installed on a central EC2