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.passapply.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 Devops team is currently looking at the security aspect of their CI/CD pipeline. They are making use of AWS resource? for their infrastructure. They want to ensure that the EC2 Instances don\'t have any high security vulnerabilities. They want to ensure a complete DevSecOps process. How can this be achieved?

Please select:

A. Use AWS Config to check the state of the EC2 instance for any sort of security issues.

B. Use AWS Inspector API\\'s in the pipeline for the EC2 Instances

C. Use AWS Trusted Advisor API\\'s in the pipeline for the EC2 Instances

D. Use AWS Security Groups to ensure no vulnerabilities are present

Correct Answer: B

Amazon Inspector offers a programmatic way to find security defects or misconfigurations in your operating systems and applications. Because you can use API calls to access both the processing of assessments and the results of your assessments, integration of the findings into workflow and notification systems is simple. DevOps teams can integrate Amazon Inspector into their CI/CD pipelines and use it to identify any pre- existing issues or when new issues are introduced. Option A.C and D are all incorrect since these services cannot check for Security Vulnerabilities. These can only be checked by the AWS Inspector service. For more information on AWS Security best practices, please refer to below URL: https://d1.awsstatic.com/whitepapers/Security/AWS Security Best Practices.pdl The correct answer is: Use AWS Inspector API\\'s in the pipeline for the EC2 Instances

QUESTION 2

An organizational must establish the ability to delete an AWS KMS Customer Master Key (CMK) within a 24-hour timeframe to keep it from being used for encrypt or decrypt operations.

Which of the following actions will address this requirement?

A. Manually rotate a key within KMS to create a new CMK immediately

B. Use the KMS import key functionality to execute a delete key operation

C. Use the schedule key deletion function within KMS to specify the minimum wait period for deletion

D. Change the KMS CMK alias to immediately prevent any services from using the CMK.

Correct Answer: C

Reference: https://docs.aws.amazon.com/kms/latest/developerguide/deleting-keys.html

QUESTION 3

A company has an encrypted Amazon S3 bucket. An Application Developer has an IAM policy that allows access to the S3 bucket, but the Application Developer is unable to access objects within the bucket. What is a possible cause of the issue?

A. The S3 ACL for the S3 bucket fails to explicitly grant access to the Application Developer

B. The AWS KMS key for the S3 bucket fails to list the Application Developer as an administrator

C. The S3 bucket policy fails to explicitly grant access to the Application Developer

D. The S3 bucket policy explicitly denies access to the Application Developer

Correct Answer: C

QUESTION 4

A company uses Microsoft Active Directory for access management for on-premises resources and wants to use the same mechanism for accessing its AWS accounts. Additionally, the development team plans to launch a public-facing application for which they need a separate authentication solution.

When coma nation of the following would satisfy these requirements? (Select TWO)

A. Set up domain controllers on Amazon EC2 to extend the on-premises directory to AWS

B. Establish network connectivity between on-premises and the user\\'s VPC

C. Use Amazon Cognito user pools for application authentication

D. Use AD Connector tor application authentication.

E. Set up federated sign-in to AWS through ADFS and SAML.

Correct Answer: AB

QUESTION 5

A company has multiple accounts in the AWS Cloud. Users in the developer account need to have access to specific resources in the production account.

What is the MOST secure way to provide this access?

A. Create one IAM user in the production account. Grant the appropriate permissions to the resources that are needed. Share the password only with the users that need access.

B. Create cross-account access with an IAM role in the developer account. Grant the appropriate permissions to this role. Allow users in the developer account to assume this role to access the production resources.

C. Create cross-account access with an IAM user account in the production account. Grant the appropriate permissions to this user account. Allow users in the developer account to use this user account to access the production resources.

D. Create cross-account access with an IAM role in the production account. Grant the appropriate permissions to this role. Allow users in the developer account to assume this role to access the production resources.

Correct Answer: A

Latest SCS-C01 Dumps   SCS-C01 VCE Dumps   SCS-C01 Practice Test