SCS-C02 Q&As

AWS Certified Security - Specialty

QUESTION 1

A company requires that SSH commands used to access its IAM instance be traceable to the user who executed each command. How should a Security Engineer accomplish this?

A. Allow inbound access on port 22 at the security group attached to the instance Use IAM Systems Manager Session Manager for shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch togging tor Systems Manager sessions

B. Use Amazon S3 to securely store one Privacy Enhanced Mail Certificate (PEM file) for each user Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on port 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance

C. Deny inbound access on port 22 at the security group attached to the instance Use IAM Systems Manager Session Manager tor shell access to Amazon EC2 instances with the user tag defined Enable Amazon CloudWatch togging for Systems Manager sessions

D. Use Amazon S3 to securely store one Privacy Enhanced Mall Certificate (PEM fie) for each team or group Allow Amazon EC2 to read from Amazon S3 and import every user that wants to use SSH to access EC2 instances Allow inbound access on pod 22 at the security group attached to the instance Install the Amazon CloudWatch agent on the EC2 instance and configure it to ingest audit logs for the instance

Correct Answer: C

QUESTION 2

A company\\'s security team has defined a set of IAM Config rules that must be enforced globally in all IAM accounts the company owns. What should be done to provide a consolidated compliance overview for the security team?

A. Use IAM Organizations to limit IAM Config rules to the appropriate Regions, and then consolidate the Amazon CloudWatch dashboard into one IAM account.

B. Use IAM Config aggregation to consolidate the views into one IAM account, and provide role access to the security team.

C. Consolidate IAM Config rule results with an IAM Lambda function and push data to Amazon SQS. Use Amazon SNS to consolidate and alert when some metrics are triggered.

D. Use Amazon GuardDuty to load data results from the IAM Config rules compliance status, aggregate GuardDuty findings of all IAM accounts into one IAM account, and provide role access to the security team.

Correct Answer: B

QUESTION 3

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

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

QUESTION 4

A company\\'s engineering team is developing a new application that creates IAM Key Management Service (IAM KMS) CMK grants for users immediately after a grant IS created users must be able to use the CMK tu encrypt a 512-byte payload. During load testing, a bug appears |intermittently where AccessDeniedExceptions are occasionally triggered when a user rst attempts to encrypt using the CMK

Which solution should the c0mpany`s security specialist recommend`?

A. Instruct users to implement a retry mechanism every 2 minutes until the call succeeds.

B. Instruct the engineering team to consume a random grant token from users, and to call the CreateGrant operation, passing it the grant token. Instruct use to use that grant token in their call to encrypt.

C. Instruct the engineering team to create a random name for the grant when calling the CreateGrant operation. Return the name to the users and instruct them to provide the name as the grant token in the call to encrypt.

D. Instruct the engineering team to pass the grant token returned in the CreateGrant response to users. Instruct users to use that grant token in their call to encrypt.

Correct Answer: D

QUESTION 5

Due to new compliance requirements, a Security Engineer must enable encryption with customer-provided keys on corporate data that is stored in DynamoDB. The company wants to retain full control of the encryption keys.

Which DynamoDB feature should the Engineer use to achieve compliance\\'?

A. Use IAM Certificate Manager to request a certificate. Use that certificate to encrypt data prior to uploading it to DynamoDB.

B. Enable S3 server-side encryption with the customer-provided keys. Upload the data to Amazon S3, and then use S3Copy to move all data to DynamoDB

C. Create a KMS master key. Generate per-record data keys and use them to encrypt data prior to uploading it to

DynamoDS. Dispose of the cleartext and encrypted data keys after encryption without storing.

D. Use the DynamoDB Java encryption client to encrypt data prior to uploading it to DynamoDB.

Correct Answer: D

Follow the link: https://docs.IAM.amazon.com/dynamodb-encryption- client/latest/devguide/what-is-ddb-encrypt.html