



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.pass4itsure.com/scs-c02.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 is building an application on IAM that will store sensitive Information. The company has a support team with access to the IT infrastructure, including databases. The company's security engineer must introduce measures to protect the sensitive data against any data breach while minimizing management overhead. The credentials must be regularly rotated.

What should the security engineer recommend?

- A. Enable Amazon RDS encryption to encrypt the database and snapshots. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instances. Include the database credential in the EC2 user data field. Use an IAM Lambda function to rotate database credentials. Set up TLS for the connection to the database.
- B. Install a database on an Amazon EC2 Instance. Enable third-party disk encryption to encrypt the Amazon Elastic Block Store (Amazon EBS) volume. Store the database credentials in IAM CloudHSM with automatic rotation. Set up TLS for the connection to the database.
- C. Enable Amazon RDS encryption to encrypt the database and snapshots. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instances. Store the database credentials in IAM Secrets Manager with automatic rotation. Set up TLS for the connection to the RDS hosted database.
- D. Set up an IAM CloudHSM cluster with IAM Key Management Service (IAM KMS) to store KMS keys. Set up Amazon RDS encryption using IAM KMS to encrypt the database. Store database credentials in the IAM Systems Manager Parameter Store with automatic rotation. Set up TLS for the connection to the RDS hosted database.

Correct Answer: C

To protect the sensitive data against any data breach and minimize management overhead, the security engineer should recommend the following solution: Enable Amazon RDS encryption to encrypt the database and snapshots. This allows the security engineer to use AWS Key Management Service (AWS KMS) to encrypt data at rest for the database and any backups or replicas. Enable Amazon Elastic Block Store (Amazon EBS) encryption on Amazon EC2 instances. This allows the security engineer to use AWS KMS to encrypt data at rest for the EC2 instances and any snapshots or volumes. Store the database credentials in AWS Secrets Manager with automatic rotation. This allows the security engineer to encrypt and manage secrets centrally, and to configure automatic rotation schedules for them. Set up TLS for the connection to the RDS hosted database. This allows the security engineer to encrypt data in transit between the EC2 instances and the database.

QUESTION 2

A company has an AWS account that hosts a production application. The company receives an email notification that Amazon GuardDuty has detected an Impact:IAMUser/AnomalousBehavior finding in the account. A security engineer needs to run the investigation playbook for this security incident and must collect and analyze the information without affecting the application.

Which solution will meet these requirements MOST quickly?

- A. Log in to the AWS account by using read-only credentials. Review the GuardDuty finding for details about the IAM credentials that were used. Use the IAM console to add a DenyAll policy to the IAM principal.
- B. Log in to the AWS account by using read-only credentials. Review the GuardDuty finding to determine which API calls initiated the finding. Use Amazon Detective to review the API calls in context.
- C. Log in to the AWS account by using administrator credentials. Review the GuardDuty finding for details about the



IAM credentials that were used. Use the IAM console to add a DenyAll policy to the IAM principal.

D. Log in to the AWS account by using read-only credentials. Review the GuardDuty finding to determine which API calls initiated the finding. Use AWS CloudTrail Insights and AWS CloudTrail Lake to review the API calls in context.

Correct Answer: B

This answer is correct because logging in with read-only credentials minimizes the risk of accidental or malicious changes to the AWS account. Reviewing the GuardDuty finding can help identify which API calls initiated the finding and which IAM principal was involved. Using Amazon Detective can help analyze and visualize the API calls in context, such as which resources were affected, which IP addresses were used, and how the activity deviated from normal patterns. Amazon Detective can also help identify related findings from other sources, such as AWS Config or AWS Audit Manager.

QUESTION 3

A security engineer needs to create an IAM Key Management Service