

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.leads4pass.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 security engineer configures Amazon S3 Cross-Region Replication (CRR) for all objects that are in an S3 bucket in the us-east-1. Region Some objects in this S3 bucket use server-side encryption with AWS KMS keys (SSE-KMS) for encryption at rest. The security engineer creates a destination S3 bucket in the us-west-2 Region. The destination S3 bucket is in the same AWS account as the source S3 bucket.

The security engineer also creates a customer managed key in us-west-2 to encrypt objects at rest in the destination S3 bucket. The replication configuration is set to use the key in us-west-2 to encrypt objects in the destination S3 bucket. The security engineer has provided the S3 replication configuration with an IAM role to perform the replication in Amazon S3.

After a day, the security engineer notices that no encrypted objects from the source S3 bucket are replicated to the destination S3 bucket. However, all the unencrypted objects are replicated.

Which combination of steps should the security engineer take to remediate this issue? (Select THREE.)

- A. Change the replication configuration to use the key in us-east-1 to encrypt the objects that are in the destination S3 bucket.
- B. Grant the IAM role the kms. Encrypt permission for the key in us-east-1 that encrypts source objects.
- C. Grant the IAM role the s3 GetObjectVersionForReplication permission for objects that are in the source S3 bucket.
- D. Grant the IAM role the kms. Decrypt permission for the key in us-east-1 that encrypts source objects.
- E. Change the key policy of the key in us-east-1 to grant the kms. Decrypt permission to the security engineer's IAM account.
- F. Grant the IAM role the kms Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket.

Correct Answer: BF

To enable S3 Cross-Region Replication (CRR) for objects that are encrypted with SSE-KMS, the following steps are required:

Grant the IAM role the kms.Decrypt permission for the key in us-east-1 that encrypts source objects. This will allow the IAM role to decrypt the source objects before replicating them to the destination bucket. The kms.Decrypt permission must

be granted in the key policy of the source KMS key or in an IAM policy attached to the IAM role.

Grant the IAM role the kms.Encrypt permission for the key in us-west-2 that encrypts objects that are in the destination S3 bucket. This will allow the IAM role to encrypt the replica objects with the destination KMS key before storing them in

the destination bucket. The kms.Encrypt permission must be granted in the key policy of the destination KMS key or in an IAM policy attached to the IAM role. This solution will remediate the issue of encrypted objects not being replicated to

the destination bucket.

The other options are incorrect because they either do not grant the necessary permissions for CRR (A, C, D), or do not use a valid encryption method for CRR (E).

Verified References:

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/replication-config-for-kms-objects.html>

QUESTION 2

A company has an encrypted Amazon Aurora DB cluster in the us-east-1 Region. The DB cluster is encrypted with an AWS Key Management Service (AWS KMS) customer managed key. To meet compliance requirements, the company needs to copy a DB snapshot to the us-west-1 Region. However, when the company tries to copy the snapshot to us-west-1 the company cannot access the key that was used to encrypt the original database.

What should the company do to set up the snapshot in us-west-1 with proper encryption?

- A. Use AWS Secrets Manager to store the customer managed key in us-west-1 as a secret Use this secret to encrypt the snapshot in us-west-1.
- B. Create a new customer managed key in us-west-1. Use this new key to encrypt the snapshot in us-west-1.
- C. Create an IAM policy that allows access to the customer managed key in us-east-1. Specify `arn:aws:kms:us-west-1:*` as the principal.
- D. Create an IAM policy that allows access to the customer managed key in us-east-1. Specify `arn:aws:rds:us-west-1:*` as the principal.

Correct Answer: B

"If you copy an encrypted snapshot across Regions, you must specify a KMS key valid in the destination AWS Region. It can be a Region-specific KMS key, or a multi-Region key." <https://docs.aws.amazon.com/AmazonRDS/latest/AuroraUserGuide/aurora-copy-snapshot.html#aurora-copy-snapshot.Encryption>

QUESTION 3

A company is implementing a new application in a new IAM account. A VPC and subnets have been created for the application. The application has been peered to an existing VPC in another account in the same IAM Region for database access. Amazon EC2 instances will regularly be created and terminated in the application VPC, but only some of them will need access to the databases in the peered VPC over TCP port 1521. A security engineer must ensure that only the EC2 instances that need access to the databases can access them through the network.

How can the security engineer implement this solution?

- A. Create a new security group in the database VPC and create an inbound rule that allows all traffic from the IP address range of the application VPC. Add a new network ACL rule on the database subnets. Configure the rule to TCP port 1521 from the IP address range of the application VPC. Attach the new security group to the database instances that the application instances need to access.
- B. Create a new security group in the application VPC with an inbound rule that allows the IP address range of the database VPC over TCP port 1521. Create a new security group in the database VPC with an inbound rule that allows the IP address range of the application VPC over port 1521. Attach the new security group to the database instances and the application instances that need database access.
- C. Create a new security group in the application VPC with no inbound rules. Create a new security group in the database VPC with an inbound rule that allows TCP port 1521 from the new application security group in the application VPC. Attach the application security group to the application instances that need database access, and attach the

database security group to the database instances.

D. Create a new security group in the application VPC with an inbound rule that allows the IP address range of the database VPC over TCP port 1521. Add a new network ACL rule on the database subnets. Configure the rule to allow all traffic from the IP address range of the application VPC. Attach the new security group to the application instances that need database access.

Correct Answer: C

QUESTION 4

A company that uses AWS Organizations wants to see AWS Security Hub findings for many AWS accounts and AWS Regions. Some of the accounts are in the company's organization, and some accounts are in organizations that the company manages for customers. Although the company can see findings in the Security Hub administrator account for accounts in the company's organization, there are no findings from accounts in other organizations.

Which combination of steps should the company take to see findings from accounts that are outside the organization that includes the Security Hub administrator account? (Select TWO.)

- A. Use a designated administration account to automatically set up member accounts.
- B. Create the AWS Service Role ForSecurity Hub service-linked role for Security Hub.
- C. Send an administration request from the member accounts.
- D. Enable Security Hub for all member accounts.
- E. Send invitations to accounts that are outside the company's organization from the Security Hub administrator account.

Correct Answer: CE

To see Security Hub findings for accounts that are outside the organization that includes the Security Hub administrator account, the following steps are required: Send invitations to accounts that are outside the company's organization from the Security Hub administrator account. This will allow the administrator account to view and manage findings from those accounts. The administrator account can send invitations by using the Security Hub console, API, or CLI. For more information, see [Sending invitations to member accounts](#). Send an administration request from the member accounts. This will allow the member accounts to accept the invitation from the administrator account and establish a relationship with it. The member accounts can send administration requests by using the Security Hub console, API, or CLI. For more information, see [Sending administration requests](#). This solution will enable the company to see Security Hub findings for many AWS accounts and AWS Regions, including accounts that are outside its own organization. The other options are incorrect because they either do not establish a relationship between the administrator and member accounts (A, B), do not enable Security Hub for all member accounts (D), or do not use a valid service for Security Hub (F). Verified References: <https://docs.aws.amazon.com/securityhub/latest/userguide/securityhub-member-accounts.html>

QUESTION 5

What are the MOST secure ways to protect the AWS account root user of a recently opened AWS account? (Select TWO.)

- A. Use the AWS account root user access keys instead of the AWS Management Console.

- B. Enable multi-factor authentication for the AWS IAM users with the Adminis-tratorAccess managed policy attached to them.
- C. Enable multi-factor authentication for the AWS account root user.
- D. Use AWS KMS to encrypt all AWS account root user and AWS IAM access keys and set automatic rotation to 30 days.
- E. Do not create access keys for the AWS account root user; instead, create AWS IAM users.

Correct Answer: CE

[Latest SCS-C02 Dumps](#)

[SCS-C02 VCE Dumps](#)

[SCS-C02 Braindumps](#)