



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.passapply.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 team is using Amazon EC2 Image Builder to build a hardened AMI with forensic capabilities. An AWS Key Management Service (AWS KMS) key will encrypt the forensic AMI. EC2 Image Builder successfully installs the required patches and packages in the security team's AWS account. The security team uses a federated IAM role in the same AWS account to sign in to the AWS Management Console and attempts to launch the forensic AMI. The EC2 instance launches and immediately terminates.

What should the security team do to launch the EC2 instance successfully?

- A. Update the policy that is associated with the federated IAM role to allow the `ec2:DescribeImages` action for the forensic AMI.
- B. Update the policy that is associated with the federated IAM role to allow the `ec2:StartInstances` action in the security team's AWS account.
- C. Update the policy that is associated with the KMS key that is used to encrypt the forensic AMI. Configure the policy to allow the `kms:Encrypt` and `kms:Decrypt` actions for the federated IAM role.
- D. Update the policy that is associated with the federated IAM role to allow the `kms:DescribeKey` action for the KMS key that is used to encrypt the forensic AMI.

Correct Answer: C

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/troubleshooting-launch.html#troubleshooting-launch-internal>

QUESTION 2

A company is running an application in the eu-west-1 Region. The application uses an IAM Key Management Service (IAM KMS) CMK to encrypt sensitive data. The company plans to deploy the application in the eu-north-1 Region.

A security engineer needs to implement a key management solution for the application deployment in the new Region. The security engineer must minimize changes to the application code.

Which change should the security engineer make to the IAM KMS configuration to meet these requirements?

- A. Update the key policies in eu-west-1. Point the application in eu-north-1 to use the same CMK as the application in eu-west-1.
- B. Allocate a new CMK to eu-north-1 to be used by the application that is deployed in that Region.
- C. Allocate a new CMK to eu-north-1. Create the same alias name for both keys. Configure the application deployment to use the key alias.
- D. Allocate a new CMK to eu-north-1. Create an alias for eu-north-1. Change the application code to point to the alias for eu-north-1.

Correct Answer: B

QUESTION 3



A security administrator is setting up a new AWS account. The security administrator wants to secure the data that a company stores in an Amazon S3 bucket. The security administrator also wants to reduce the chance of unintended data exposure and the potential for misconfiguration of objects that are in the S3 bucket.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Configure the S3 Block Public Access feature for the AWS account.
- B. Configure the S3 Block Public Access feature for all objects that are in the bucket.
- C. Deactivate ACLs for objects that are in the bucket.
- D. Use AWS PrivateLink for Amazon S3 to access the bucket.

Correct Answer: D

QUESTION 4

A company uses Amazon RDS for MySQL as a database engine for its applications. A recent security audit revealed an RDS instance that is not compliant with company policy for encrypting data at rest. A security engineer at the company needs to ensure that all existing RDS databases are encrypted using server-side encryption and that any future deviations from the policy are detected.

Which combination of steps should the security engineer take to accomplish this? (Select TWO.)

- A. Create an IAM Config rule to detect the creation of unencrypted RDS databases. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to trigger on the IAM Config rules compliance state change and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.
- B. Use IAM System Manager State Manager to detect RDS database encryption configuration drift. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to track state changes and use Amazon Simple Notification Service (Amazon SNS) to notify the security operations team.
- C. Create a read replica for the existing unencrypted RDS database and enable replica encryption in the process. Once the replica becomes active, promote it into a standalone database instance and terminate the unencrypted database instance.
- D. Take a snapshot of the unencrypted RDS database. Copy the snapshot and enable snapshot encryption in the process. Restore the database instance from the newly created encrypted snapshot. Terminate the unencrypted database instance.
- E. Enable encryption for the identified unencrypted RDS instance by changing the configurations of the existing database

Correct Answer: AD

QUESTION 5

A company hosts a public website on an Amazon EC2 instance. HTTPS traffic must be able to access the website. The company uses SSH for management of the web server.

The website is on the subnet 10.0.1.0/24. The management subnet is 192.168.100.0/24. A security engineer must create a security group for the EC2 instance.



Which combination of steps should the security engineer take to meet these requirements in the MOST secure manner? (Select TWO.)

- A. Allow port 22 from source 0.0.0.0/0.
- B. Allow port 443 from source 0.0.0.0/0.
- C. Allow port 22 from 192.168.100.0/24.
- D. Allow port 22 from 10.0.1.0/24.
- E. Allow port 443 from 10.0.1.0/24.

Correct Answer: BC

The correct answer is B and C.

- B. Allow port 443 from source 0.0.0.0/0.

This is correct because port 443 is used for HTTPS traffic, which must be able to access the website from any source IP address.

- C. Allow port 22 from 192.168.100.0/24.

This is correct because port 22 is used for SSH, which is the management protocol for the web server. The management subnet is 192.168.100.0/24, so only this subnet should be allowed to access port 22.

- A. Allow port 22 from source 0.0.0.0/0.

This is incorrect because it would allow anyone to access port 22, which is a security risk. SSH should be restricted to the management subnet only.

- D. Allow port 22 from 10.0.1.0/24.

This is incorrect because it would allow the website subnet to access port 22, which is unnecessary and a security risk. SSH should be restricted to the management subnet only.

- E. Allow port 443 from 10.0.1.0/24.

This is incorrect because it would limit the HTTPS traffic to the website subnet only, which defeats the purpose of having a public website.

[SCS-C02 Practice Test](#)

[SCS-C02 Study Guide](#)

[SCS-C02 Braindumps](#)