



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.geekcert.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 stores critical data in an S3 bucket. There is a requirement to ensure that an extra level of security is added to the S3 bucket. In addition, it should be ensured that objects are available in a secondary region if the primary one goes down. Which of the following can help fulfil these requirements? Choose 2 answers from the options given below

- A. Enable bucket versioning and also enable CRR
- B. Enable bucket versioning and enable Master Pays
- C. For the Bucket policy add a condition for `{"Null": {"IAM:MultiFactorAuthAge": true}}`
- D. Enable the Bucket ACL and add a condition for `{"Null": {"IAM:MultiFactorAuthAge": true}}`

Correct Answer: AC

The IAM Documentation mentions the following Adding a Bucket Policy to Require MFA Amazon S3 supports MFA-protected API access, a feature that can enforce multi-factor authentication (MFA) for access to your Amazon S3 resources. Multi-factor authentication provides an extra level of security you can apply to your IAM environment. It is a security feature that requires users to prove physical possession of an MFA device by providing a valid MFA code. For more information, go to IAM Multi-Factor Authentication. You can require MFA authentication for any requests to access your Amazon S3 resources. You can enforce the MFA authentication requirement using the `IAM:MultiFactorAuthAge` key in a bucket policy. IAM users can access Amazon S3 resources by using temporary credentials issued by the IAM Security Token Service (STS). You provide the MFA code at the time of the STS request. When Amazon S3 receives a request with MFA authentication, the `IAM:MultiFactorAuthAge` key provides a numeric value indicating how long ago (in seconds) the temporary credential was created. If the temporary credential provided in the request was not created using an MFA device, this key value is null (absent). In a bucket policy, you can add a condition to check this value, as shown in the following example bucket policy. The policy denies any Amazon S3 operation on the `/taxdocuments` folder in the `examplebucket` bucket if the request is not MFA authenticated. To learn more about MFA authentication, see Using Multi-Factor Authentication (MFA) in IAM in the IAM User Guide.



```
{
  "Version": "2012-10-17",
  "Id": "123",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::examplebucket/taxdocuments/*",
      "Condition": { "Null": { "aws:MultiFactorAuthAge": true } }
    }
  ]
}
```

Option B is invalid because just enabling bucket versioning will not guarantee replication of objects Option D is invalid because the condition for the bucket policy needs to be set accordingly For more information on example bucket policies, please visit the following URL: <https://docs.IAM.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html> Also versioning and Cross Region replication can ensure that objects will be available in the destination region in case the primary region fails. For more information on CRR, please visit the following URL: <https://docs.IAM.amazon.com/AmazonS3/latest/dev/crr.html> The correct answers are: Enable bucket versioning and also enable CRR, For the Bucket policy add a condition for {"Null": { "IAM:MultiFactorAuthAge": true}} Submit your Feedback/ Queries to our Experts

QUESTION 2

A Systems Engineer is troubleshooting the connectivity of a test environment that includes a virtual security appliance deployed inline. In addition to using the virtual security appliance, the Development team wants to use security groups and network ACLs to accomplish various security requirements in the environment.

What configuration is necessary to allow the virtual security appliance to route the traffic?

- A. Disable network ACLs.
- B. Configure the security appliance's elastic network interface for promiscuous mode.
- C. Disable the Network Source/Destination check on the security appliance's elastic network interface
- D. Place the security appliance in the public subnet with the internet gateway

Correct Answer: C



Each EC2 instance performs source/destination checks by default. This means that the instance must be the source or destination of any traffic it sends or receives. In this case virtual security appliance instance must be able to send and receive traffic when the source or destination is not itself. Therefore, you must disable source/destination checks on the NAT instance."

QUESTION 3

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? (Choose 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

QUESTION 4

A company has a web-based application using Amazon CloudFront and running on Amazon Elastic Container Service (Amazon ECS) behind an Application Load Balancer (ALB). The ALB is terminating TLS and balancing load across ECS

service tasks A security engineer needs to design a solution to ensure that application content is accessible only through CloudFront and that it is never accessible directly.

How should the security engineer build the MOST secure solution?

- A. Add an origin custom header Set the viewer protocol policy to HTTP and HTTPS Set the origin protocol policy to HTTPS only Update the application to validate the CloudFront custom header
- B. Add an origin custom header Set the viewer protocol policy to HTTPS only Set the origin protocol policy to match viewer Update the application to validate the CloudFront custom header.
- C. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTPS Set the origin protocol policy to HTTP only Update the application to validate the CloudFront custom header.
- D. Add an origin custom header Set the viewer protocol policy to redirect HTTP to HTTPS. Set the origin protocol policy to HTTPS only Update the application to validate the CloudFront custom header

Correct Answer: D

**QUESTION 5**

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>

[SCS-C02 VCE Dumps](#)

[SCS-C02 Practice Test](#)

[SCS-C02 Exam Questions](#)