



# SCS-C02<sup>Q&As</sup>

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 hosts data in S3. There is a requirement to control access to the S3 buckets. Which are the 2 ways in which this can be achieved?

- A. Use Bucket policies
- B. Use the Secure Token service
- C. Use IAM user policies
- D. Use IAM Access Keys

Correct Answer: AC

The IAM Documentation mentions the following Amazon S3 offers access policy options broadly categorized as resource-based policies and user policies. Access policies you attach to your resources (buckets and objects) are referred to as resource-based policies. For example, bucket policies and access control lists (ACLs) are resource-based policies. You can also attach access policies to users in your account. These are called user policies. You may choose to use resource-based policies, user policies, or some combination of these to manage permissions to your Amazon S3 resources. Option B and D are invalid because these cannot be used to control access to S3 buckets For more information on S3 access control, please refer to the below Link:

<https://docs.IAM.amazon.com/AmazonS3/latest/dev/s3-access-control.html> The correct answers are: Use Bucket policies. Use IAM user policies Submit your Feedback/Queries to our Experts

### QUESTION 2

Your company use IAM KMS for management of its customer keys. From time to time, there is a requirement to delete existing keys as part of housekeeping activities. What can be done during the deletion process to verify that the key is no longer being used?

- A. Use CloudTrail to see if any KMS API request has been issued against existing keys
- B. Use Key policies to see the access level for the keys
- C. Rotate the keys once before deletion to see if other services are using the keys
- D. Change the IAM policy for the keys to see if other services are using the keys

Correct Answer: A

The IAM lentionation mentions the following You can use a combination of IAM CloudTrail, Amazon CloudWatch Logs, and Amazon Simple Notification Service (Amazon SNS) to create an alarm that notifies you of IAM KMS API requests that attempt to use a customer master key (CMK) that is pending deletion. If you receive a notification from such an alarm, you might want to cancel deletion of the CMK to give yourself more time to determine whether you want to delete it Options B and D are incorrect because Key policies nor IAM policies can be used to check if the keys are being used. Option C is incorrect since rotation will not help you check if the keys are being used. For more information on deleting keys, please refer to below URL: <https://docs.IAM.amazon.com/kms/latest/developereuide/deletine-keys-creatine-cloudwatch-alarm.html> The correct answer is: Use CloudTrail to see if any KMS API request has been issued against existing keys Submit your Feedback/Queries to our Experts

**QUESTION 3**

You have an EBS volume attached to an EC2 Instance which uses KMS for Encryption. Someone has now gone ahead and deleted the Customer Key which was used for the EBS encryption. What should be done to ensure the data can be decrypted?

- A. Create a new Customer Key using KMS and attach it to the existing volume
- B. You cannot decrypt the data that was encrypted under the CMK, and the data is not recoverable.
- C. Request IAM Support to recover the key
- D. Use IAM Config to recover the key

Correct Answer: B

Deleting a customer master key (CMK) in IAM Key Management Service (IAM KMS) is destructive and potentially dangerous. It deletes the key material and all metadata associated with the CMK, and is irreversible. After a CMK is deleted you can no longer decrypt the data that was encrypted under that CMK, which means that data becomes unrecoverable. You should delete a CMK only when you are sure that you don't need to use it anymore. If you are not sure, consider disabling the CMK instead of deleting it. You can re-enable a disabled CMK if you need to use it again later, but you cannot recover a deleted CMK. <https://docs.IAM.amazon.com/kms/latest/developerguide/deleting-keys.html> A is incorrect because Creating a new CMK and attaching it to the exiting volume will not allow the data to be decrypted, you cannot attach customer master keys after the volume is encrypted Option C and D are invalid because once the key has been deleted, you cannot recover it For more information on EBS Encryption with KMS, please visit the following URL: <https://docs.IAM.amazon.com/kms/latest/developerguide/services-ebs.html> The correct answer is: You cannot decrypt the data that was encrypted under the CMK, and the data is not recoverable. Submit your Feedback/Queries to our Experts

---

**QUESTION 4**

A Security Engineer has been asked to troubleshoot inbound connectivity to a web server. This single web server is not receiving inbound connections from the internet, whereas all other web servers are functioning properly.

The architecture includes network ACLs, security groups, and a virtual security appliance. In addition, the Development team has implemented Application Load Balancers (ALBs) to distribute the load across all web servers. It is a

requirement that traffic between the web servers and the internet flow through the virtual security appliance.

The Security Engineer has verified the following:

1.

The rule set in the Security Groups is correct

2.

The rule set in the network ACLs is correct

3.

The rule set in the virtual appliance is correct

Which of the following are other valid items to troubleshoot in this scenario? (Choose two.)



- A. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to a NAT gateway.
- B. Verify which Security Group is applied to the particular web server's elastic network interface (ENI).
- C. Verify that the 0.0.0.0/0 route in the route table for the web server subnet points to the virtual security appliance.
- D. Verify the registered targets in the ALB.
- E. Verify that the 0.0.0.0/0 route in the public subnet points to a NAT gateway.

Correct Answer: CD

<https://docs.IAM.amazon.com/IAMEC2/latest/UserGuide/using-eni.html>

## QUESTION 5

A security engineer receives a notice from the AWS Abuse team about suspicious activity from a Linux-based Amazon EC2 instance that uses Amazon Elastic Block Store (Amazon EBS)-based storage. The instance is making connections to known malicious addresses.

The instance is in a development account within a VPC that is in the us-east-1 Region. The VPC contains an internet gateway and has a subnet in us-east-1a and us-east-1b. Each subnet is associated with a route table that uses the internet gateway as a default route. Each subnet also uses the default network ACL. The suspicious EC2 instance runs within the us-east-1b subnet. During an initial investigation, a security engineer discovers that the suspicious instance is the only instance that runs in the subnet.

Which response will immediately mitigate the attack and help investigate the root cause?

- A. Log in to the suspicious instance and use the netstat command to identify remote connections. Use the IP addresses from these remote connections to create deny rules in the security group of the instance. Install diagnostic tools on the instance for investigation. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule during the investigation of the instance.
- B. Update the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule. Replace the security group with a new security group that allows connections only from a diagnostics security group. Update the outbound network ACL for the us-east-1b subnet to remove the deny all rule. Launch a new EC2 instance that has diagnostic tools. Assign the new security group to the new EC2 instance. Use the new EC2 instance to investigate the suspicious instance.
- C. Ensure that the Amazon Elastic Block Store (Amazon EBS) volumes that are attached to the suspicious EC2 instance will not delete upon termination. Terminate the instance. Launch a new EC2 instance in us-east-1a that has diagnostic tools. Mount the EBS volumes from the terminated instance for investigation.
- D. Create an AWS WAF web ACL that denies traffic to and from the suspicious instance. Attach the AWS WAF web ACL to the instance to mitigate the attack. Log in to the instance and install diagnostic tools to investigate the instance.

Correct Answer: B

This option suggests updating the outbound network ACL for the subnet in us-east-1b to explicitly deny all connections as the first rule, replacing the security group with a new one that only allows connections from a diagnostics security group, and launching a new EC2 instance with diagnostic tools to investigate the suspicious instance. This option will immediately mitigate the attack and provide the necessary tools for investigation.



VCE & PDF

GeekCert.com

<https://www.geekcert.com/scs-c02.html>

2024 Latest geekcert SCS-C02 PDF and VCE dumps Download

---

[SCS-C02 VCE Dumps](#)

[SCS-C02 Practice Test](#)

[SCS-C02 Exam Questions](#)