

PRACTICE QUESTIONS

AWS

SCS-C02

AWS Certified Security - Specialty

SHARED BY [u/Snappy-Lantern-3122](#) on aiexamcerts

EDITION	Free Set 2
QUESTIONS	10
SHARED	October 15, 2026
EXAM	AWS SCS-C02, AWS Certified Security - Specialty

Shared by [u/Snappy-Lantern-3122](#) on aiexamcerts

10 practice questions for the AWS SCS-C02 exam, AWS Certified Security - Specialty, each followed by its answer and a short explanation. More free sets and the full practice exam: www.aiexamcerts.com/aws/scs-c02. Spotted a mistake? Email support@aiexamcerts.com with the exam code SCS-C02 and the question number.

1. Which configuration keeps application logs in CloudWatch Logs for a fixed number of days to meet a compliance requirement?

- A Set the log group retention period to the required number of days
- B Enable CloudTrail log file validation
- C Turn on S3 Object Lock on the CloudWatch Logs bucket
- D Attach a KMS key to the IAM role

Answer: A

CloudWatch Logs retention is a setting on each log group, and logs older than that period are deleted automatically. Log file validation checks integrity but does not control retention. CloudWatch Logs does not write to a customer bucket where Object Lock would apply, and a KMS key on a role does nothing for retention.

2. Customer managed KMS keys rotate automatically every 30 days by default.

- A True
- B False

Answer: B (False)

Automatic rotation for customer managed symmetric keys is off by default, and when you enable it the rotation happens once a year rather than every 30 days. Confusing the rotation interval is a common mistake in KMS questions.

3. Which AWS service automatically scans EC2 instances, container images in ECR, and Lambda functions for software vulnerabilities and network exposure?

- A AWS Config
- B AWS Audit Manager
- C Amazon Macie
- D Amazon Inspector

Answer: D

Inspector continuously assesses EC2 instances, ECR images, and Lambda functions for known vulnerabilities and unintended network reachability. Config checks resource configuration, Audit Manager collects compliance evidence, and Macie finds sensitive data in S3. None of them is a vulnerability scanner for those workloads.

4. GuardDuty findings are published as events to Amazon _____, which can trigger automated responses.

Answer: EventBridge (also accepted: Amazon EventBridge)

GuardDuty sends each finding to Amazon EventBridge, so a rule can start a Lambda function or Step Functions workflow for containment. Teams often build this pattern for automated response. The answer is the event bus that receives GuardDuty findings.

5. Which two CloudTrail event names indicate a change to IAM permissions? (Choose two.)

- A CreatePolicyVersion
- B GetObject
- C AttachRolePolicy
- D PutObject
- E DescribeInstances

Answer: A, C

CreatePolicyVersion creates a new version of a managed policy and AttachRolePolicy attaches a policy to a role, and both change what identities can do. GetObject and PutObject touch S3 objects, and DescribeInstances only reads EC2 state. Detection rules for IAM changes usually key on events like these.

6. A security group must allow SSH only from the corporate range 203.0.113.0/24. Which change is correct?

- A Add an inbound rule for TCP 22 from 203.0.113.0/24
- B Add an outbound rule for TCP 22 to 203.0.113.0/24
- C Open all ports in the network ACL to 0.0.0.0/0
- D Attach an Elastic IP to the bastion host

Answer: A

SSH is an inbound connection to the instance, so the inbound rule on the security group must allow TCP 22 from the corporate CIDR. An outbound rule controls traffic leaving the instance and does not admit SSH sessions. Opening the network ACL to the world and adding an Elastic IP both widen exposure.

7. Which method lets a principal in one account access a resource in another account without sharing long-term credentials?
- A Sharing the root user credentials between accounts
 - B Assuming a cross-account IAM role that the other account trusts
 - C Copying IAM users into the other account
 - D Storing access keys in a shared S3 bucket

Answer: B

A principal in the trusting account assumes a role in the resource account and receives temporary credentials, so no long-term secret crosses accounts. Sharing root credentials or copying users creates long-lived secrets. Keys stored in a shared bucket are a serious exposure.

8. S3 Bucket Keys require a separate KMS key for every object that is uploaded.
- A True
 - B False

Answer: B (False)

S3 Bucket Keys let S3 use one bucket-level KMS key to generate data keys for objects, which reduces the number of KMS requests and cost. A separate key per object is the opposite of what bucket keys do.

9. Which IAM policy condition key restricts API calls to requests that arrive through a specific VPC endpoint?
- A `aws:SourceVpce`
 - B `aws:SourceIp`
 - C `aws:UserAgent`
 - D `aws:RequestedRegion`

Answer: A

`aws:SourceVpce` matches the VPC endpoint a request came through, so a bucket or API can accept calls only from that endpoint. `aws:SourceIp` checks the client address, which is not meaningful for private endpoints. User agent and requested Region do not identify the network path.

10. An incident responder must isolate a suspicious EC2 instance. Which action is the most appropriate first step?
- A Terminate it immediately
 - B Delete the snapshots of its volumes
 - C Reboot it to clear any suspicious processes
 - D Snapshot its volumes and then move it to a quarantine security group with no inbound or outbound rules

Answer: D

Snapshotting first preserves evidence, and a quarantine security group cuts network access without destroying the instance state. Terminating the instance or deleting snapshots destroys evidence. Rebooting clears the memory that holds volatile evidence.