

PRACTICE QUESTIONS

AWS

SCS-C02

AWS Certified Security - Specialty

SHARED BY [u/Cosmic-Summit-5568](#) on aiexamcerts

EDITION	Free Set 1
QUESTIONS	10
SHARED	October 15, 2026
EXAM	AWS SCS-C02, AWS Certified Security - Specialty

Shared by [u/Cosmic-Summit-5568](#) 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. A third-party partner assumes a cross-account role in your account. Which condition key helps prevent the confused deputy problem?

- A `aws:SourceIp`
- B `aws:MultiFactorAuthPresent`
- C `sts:ExternalId`
- D `aws:PrincipalTag`

Answer: C

An external ID is a secret value the partner must present when assuming the role, so a different customer's request cannot trick the partner into using your role. Source IP and MFA conditions do not stop the confused deputy problem. Principal tags describe the caller, not the trust relationship.

2. AWS Security Hub normalizes findings from many services into the AWS Security Finding _____ (ASFF).

Answer: Format

Security Hub converts findings from GuardDuty, Inspector, Macie, and partner tools into one schema called the AWS Security Finding Format. A common schema makes it possible to search and automate across sources. The answer completes the name of that schema.

3. Which AWS service adds DDoS protection with 24/7 access to the AWS Shield Response Team for applications such as Amazon CloudFront and Application Load Balancers?

- A AWS WAF only
- B AWS Shield Standard
- C AWS Network Firewall
- D AWS Shield Advanced

Answer: D

Shield Advanced adds enhanced detection, cost protection, and access to the Shield Response Team for protected resources. Shield Standard is automatic but does not include the response team. WAF and Network Firewall filter traffic but do not provide the DDoS response service.

4. Amazon CloudWatch Logs can export log groups to Amazon S3 for long-term archival.
- A True
 - B False

Answer: A (True)

CloudWatch Logs supports exporting log data to an S3 bucket, which is a common way to archive logs cheaply. Logs can also be streamed to S3 through a subscription filter and Firehose for continuous delivery.

5. Which two controls help enforce a security baseline across many AWS accounts? (Choose two.)
- A AWS Control Tower guardrails
 - B Creating IAM users by hand in every account
 - C Service control policies in AWS Organizations
 - D Amazon Inspector scans
 - E AWS Artifact reports

Answer: A, C

Control Tower guardrails are preventive or detective rules applied across a landing zone, and SCPs enforce permission limits across an organization. Manual per-account IAM users do not scale or enforce anything consistently. Inspector scans report vulnerabilities and Artifact reports supply compliance documents, so neither enforces a baseline.

6. Instances in a VPC without internet access must reach Amazon S3 privately. Which option fits best?
- A A NAT gateway
 - B A gateway VPC endpoint for S3 with a route table entry
 - C An AWS Direct Connect public virtual interface
 - D An internet gateway with a bucket policy only

Answer: B

A gateway VPC endpoint for S3 adds a route table entry so S3 traffic stays on the AWS network with no internet path. A NAT gateway needs an internet route, which the scenario rules out. A Direct Connect public virtual interface still uses public AWS addresses, and an internet gateway would give the instances an internet path.

7. Which policy feature limits which tags a principal can change on resources?

- A A resource-based policy
- B A permissions boundary
- C A condition block that uses `aws:TagKeys` or `aws:RequestTag`
- D A service-linked role

Answer: C

Condition keys like `aws:TagKeys` and `aws:RequestTag` let a statement control which tag keys and values a principal can set, and `aws:ResourceTag` matches tags already on a resource. A resource-based policy says who can access a resource, not which tag values apply. A permissions boundary caps permissions, and a service-linked role is a role owned by an AWS service.

8. The AWS managed KMS key that EBS uses by default has the alias `aws/_____`.

Answer: ebs

The AWS managed key for EBS has the alias `aws/ebs` and is created automatically in each account and Region when you first encrypt an EBS volume. Customer managed keys give you control over the key policy and rotation. The alias name identifies the service that owns the key.

9. Which default S3 encryption option encrypts new objects with keys that S3 manages, so no KMS permissions are needed?

- A SSE-C
- B SSE-S3
- C SSE-KMS with a customer managed key
- D Client-side encryption with a local key

Answer: B

SSE-S3 uses AES-256 keys managed by S3 and needs no KMS calls or key permissions from the caller. SSE-C requires the client to send its own key with each request. SSE-KMS and client-side encryption both involve keys the caller must be able to use.

10. Which Systems Manager feature gives an incident responder an interactive shell on an instance without opening SSH?

- A Parameter Store
- B Patch Manager
- C Inventory
- D Session Manager

Answer: D

Session Manager opens an audited shell through the SSM agent, so inbound SSH ports can stay closed and sessions are logged. Parameter Store holds configuration values, Patch Manager applies patches, and Inventory collects metadata. None of them provides an interactive shell.