aws training and certification

AWS Certified Security Specialty (SCS-C01) Exam Guide

Introduction

The AWS Certified Security Specialty (SCS-C01) examination is intended for individuals who perform a security role. This exam validates an examinee's ability to effectively demonstrate knowledge about securing the AWS platform.

It validates an examinee's ability to demonstrate:

- An understanding of specialized data classifications and AWS data protection mechanisms.
- An understanding of data-encryption methods and AWS mechanisms to implement them.
- An understanding of secure Internet protocols and AWS mechanisms to implement them.
- A working knowledge of AWS security services and features of services to provide a secure production environment.
- Competency gained from two or more years of production deployment experience using AWS security services and features.
- The ability to make tradeoff decisions with regard to cost, security, and deployment complexity given a set of application requirements.
- An understanding of security operations and risks.

Examination Prerequisite

In order to take this examination, you must hold an AWS Certified foundational or role-based certification (associate or professional) in good standing.

Recommended AWS Knowledge

- A minimum of five years of IT security experience, designing and implementing security solutions.
- At least two years of hands-on experience securing AWS workloads.
- Security controls for workloads on AWS.

Exam Preparation

These training courses and materials may be helpful for examination preparation:

AWS Training (aws.amazon.com/training)

- AWS Security Fundamentals: A self-paced, online three-hour course
- Advanced Architecting on AWS: An instructor-led, live, or virtual three-day course
- Security Operations on AWS: An instructor-led, live, or virtual three-day course
- AWS Digital Training: Self-paced digital courses with modules focused on security services and topics

AWS Whitepapers (aws.amazon.com/whitepapers) Kindle and .pdf

- Security and Compliance documentation
- Compliance resources

Exam Content

Response Types

There are two types of questions on the examination:

- **Multiple-choice:** Has one correct response and three incorrect responses (distractors).
- **Multiple-response:** Has two or more correct responses out of five or more options.

Select one or more responses that best complete the statement or answer the question. Distractors, or incorrect answers, are response options that an examinee with incomplete knowledge or skill would likely choose. However, they are generally plausible responses that fit in the content area defined by the test objective.

Unanswered questions are scored as incorrect; there is no penalty for guessing.

Unscored Content

Your examination may include unscored items that are placed on the test to gather statistical information. These items are not identified on the form and do not affect your score.

Exam Results

The AWS Certified Security Specialty (SCS-C01) exam is a pass or fail exam. The examination is scored against a minimum standard established by AWS professionals who are guided by certification industry best practices and guidelines.

Your results for the examination are reported as a score from 100-1000, with a minimum passing score of 750. Your score shows how you performed on the examination as a whole and whether or not you passed. Scaled scoring models are used to equate scores across multiple exam forms that may have slightly different difficulty levels.

Your score report contains a table of classifications of your performance at each section level. This information is designed to provide general feedback concerning your examination performance. The examination uses a compensatory scoring model, which means that you do not need to "pass" the individual sections, only the overall examination. Each section of the examination has a specific weighting, so some sections have more questions than others. The table contains general information, highlighting your strengths and weaknesses. Exercise caution when interpreting section-level feedback.

Content Outline

This exam guide includes weightings, test domains, and objectives only. It is not a comprehensive listing of the content on this examination. The table below lists the main content domains and their weightings.

Domain	% of Examination
Domain 1: Incident Response	12%
Domain 2: Logging and Monitoring	20%
Domain 3: Infrastructure Security	26%
Domain 4: Identity and Access Management	20%
Domain 5: Data Protection	22%
TOTAL	**100%**

Domain 1: Incident Response

1.1 Given an AWS abuse notice, evaluate the suspected compromised instance or exposed access keys.
1.2 Verify that the Incident Response plan includes relevant AWS services.
1.3 Evaluate the configuration of automated alerting, and execute possible remediation of security-related incidents and emerging issues.

Domain 2: Logging and Monitoring

2.1 Design and implement security monitoring and alerting.
2.2 Troubleshoot security monitoring and alerting.
2.3 Design and implement a logging solution.
2.4 Troubleshoot logging solutions.

Domain 3: Infrastructure Security

3.1 Design edge security on AWS.
3.2 Design and implement a secure network infrastructure.
3.3 Troubleshoot a secure network infrastructure.
3.4 Design and implement host-based security.

Domain 4: Identity and Access Management

4.1 Design and implement a scalable authorization and authentication system to access AWS resources.
4.2 Troubleshoot an authorization and authentication system to access AWS resources.

Domain 5: Data Protection

5.1 Design and implement key management and use.
5.2 Troubleshoot key management.
5.3 Design and implement a data encryption solution for data at rest and data in transit.