# Security Specialty Exam (SCS-C01) Overview

Chandra Lingam, Cloud Wave LLC, https://www.cloudwavetraining.com/

## Introduction

"This exam validates an examinee's ability to effectively demonstrate knowledge about securing the AWS platform."

Here are some of the applied areas that you should focus

- Data Classification and Protection
- Data Encryption
- Secure Transport
- AWS Security Services

Besides, AWS expects you to have two to four years of experience using AWS offerings in the security space, ability to make the cost, security, complexity tradeoff for a given requirement, understanding security operations and risk.

This course is designed to accelerate the learning for you.

As a pre-requisite, I would recommend that you have familiarity with the AWS environment along with a certification like Cloud Practitioner or an Associate level certification.

I feel this will make the learning experience enriching, and you can immediately apply concepts that you learn in this course (in addition to passing the exam).

Let me give a brief overview of each of the above areas

## Data Classification and Protection

Here the focus is on how to protect against unintentional disclosure of data stored in AWS

Enterprises typically use a three-tier classification.

For example, from the AWS data classification whitepaper,

### Tier 1 – Protected Data

- Information for internal use
- Vendor bank account information
- Information for internal use only

### Tier 2 – Restricted Data

- Sales and marketing data, executed contracts, receipts
- Employee HR records

### Tier 3 – Highly Strategic

- Trade secret
- Pricing information
- Merger/acquisition information

- Proprietary Process
- Inventions prior to patent
- Public disclosure could cause severe or catastrophic legal, financial, or reputational damage

Depending on the classification requirement, you need to use an appropriate data protection mechanism.

The questions in the exam will spell out the classification details and type of protection required. You then need to pick the correct answer that meets the requirement.

## Data encryption

You need a good understanding of data encryption methods and how AWS implements them

For example, key management, symmetric encryption, asymmetric encryption, digital signing, encryption of data-at-rest, encryption of data in transit and so forth

## Secure Internet protocols

Secure communication protocols such as VPN, SSL/TLS, SSH (Linux/Unix client), RDP (windows client)

## AWS Security Services

AWS offers a variety of services under Identity and Access Management, Threat Detection, Configuration drift detection, Infrastructure protection, Data protection, Incident response, and so forth.

List of products are available here: https://aws.amazon.com/products/security/

You need to be familiar with the service purpose, whether it simply flags suspicious events or actively defends against attacks and so forth.

## Exam Details

The security specialty exam is 170 minutes in duration and has about 65 questions.

So, you get around two and a half minutes per question

The question format is like other AWS exams: multiple-choice or multiple responses.

In Multiple-choice questions, you need to pick one correct response from the choice given

In multiple-response questions, you need to choose two or more correct answers out of five or more options.

So, read the question carefully, and for multiple-response, it will tell you how many choices you need to pick.

In general, if you prepare well, you can quickly eliminate 50% of the choices given for a problem.

Among the remaining choices, you need to use experience and knowledge to pick one of the options.

There is no penalty for guessing – so, don't leave any question unanswered.

One or two questions may come from topics that you are not familiar with – because AWS can place unscored items in the mix to gather data.

So, if you see a question from a topic that you are not familiar with – don't panic –keep calm and pick a choice that makes the most sense and move on.

The score range is 100-1000. The passing score is **750.**

The fee for the exam is USD 300.

If you appeared for any other AWS certification, AWS issues 50% off exam vouchers for you. So, your effective fee with a voucher is USD 150.

Also, AWS has a practice exam (highly recommended). The cost is USD 40.

Once again, AWS issues a free exam voucher every time you appear for a certification exam. So, your effective cost for the practice exam with a voucher is USD 0.

If this is the first AWS certification that you are aiming for, I would recommend you start with a cloud practitioner certification. Cloud Practitioner will cover the basics, and it costs USD 100.

Appearing for the cloud practitioner exam, you will also get the 50% off exam voucher and a free practice exam voucher. So, the voucher alone will save you USD 190.

## Domains

Reference: Security Specialty Exam Guide

| Domain | Percentage of examination |
|---|---|
| Incident Response | 12% |
| Logging and Monitoring | 20% |
| Infrastructure and Security | 26% |
| Identity and Access Management | 20% |
| 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.

## Exam Preparation

Step 1: Go through all the lectures in sequence and complete all the labs and quizzes. Absorb any new information. Use the course Q&A forum if you need clarification

Step 2: Repeat lectures to fill in the gaps

Step 3: Take the exam readiness videos available in aws.training website. It has several sample questions. https://www.aws.training/Details/eLearning?id=34786

Step 4: I would recommend reading the following whitepapers:

- aws_security_incident_response.pdf
- AWS-Security-Best-Practices.pdf
- AWS-Security-Pillar.pdf

You can read them after completing all the material in this course. It will act as a good refresh.

Step 5: Take the AWS Practice Exam (use the free practice exam voucher)

Step 6: Appear for the Security Specialty Exam!

Learning is two-way, and I am there to help you. You can reach me through the course Q&A forum, and I am happy to hear from you and answer your questions.

## References

- AWS Certified Security – Specialty (SCS-C01) Exam Guide - https://aws.amazon.com/certification/certified-security-specialty/
- AWS Data Classification Whitepaper - https://d1.awsstatic.com/whitepapers/compliance/AWS_Data_Classification.pdf
- Security Products - https://aws.amazon.com/products/security/