AWS Certified Security STUDY GUIDE

SPECIALTY (SCS-C01) EXAM

Includes one year of FREE access after activation to the interactive online learning environment and study tools:

2 custom practice exams

Over 100 electronic flashcards

Searchable key term glossary

DARIO GOLDFARB, ALEXANDRE M.S.P. MORAES,
THIAGO MORAIS, MAURICIO MUÑOZ, MARCELLO ZILLO NETO,
GUSTAVO A. A. SANTANA, FERNANDO SAPATA

SYBEX
A Wiley Brand

Table of Contents

List of Tables

List of Illustrations

Chapter 1

Chapter 2

AWS Certified Security
Study Guide

Specialty (SCS-C01) Exam

**Dario Goldfarb, Alexandre M. S. P. Moraes,
Thiago Morais, Mauricio Muñoz, Marcello Zillo Neto,
Gustavo A. A. Santana, Fernando Sapata**


SYBEX
A Wiley Brand

Table of Exercises

Introduction

As the pioneer and world leader of cloud computing, Amazon Web Services (AWS) has positioned security as its highest priority. Throughout its history, the cloud provider has constantly added security-specific services to its offerings as well as security features to its ever-growing portfolio. Consequently, the AWS Certified Security–Specialty certification offers a great way for IT professionals to achieve industry recognition as cloud security experts and learn how to secure AWS environments both in concept and practice.

According to the AWS Certified Security Specialty Exam Guide, the corresponding certification attests your ability to demonstrate the following:

- 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
- The ability to make trade-off decisions with regard to cost, security, and deployment complexity given a set of application requirements
- An understanding of security operations and risks

Through multiple choice and multiple response questions, you will be tested on your ability to design, operate, and troubleshoot secure AWS architectures composed of compute, storage, networking, and monitoring services. It is expected that you know how to deal with different business objectives (such as cost optimization, agility, and regulations) to determine the best solution for a described scenario.

The AWS Certified Security–Specialty exam is intended for individuals who perform a security role with at least two years of hands-on experience securing AWS workloads.

What Does This Book Cover?

To help you prepare for the AWS Certified Security Specialty (SCS-C01) certification exam, this book explores the following topics:

Chapter 1: Security Fundamentals This chapter introduces you to basic security definitions and foundational networking concepts. It also explores major types of attacks, along with the AAA architecture, security frameworks, practical models, and other solutions. In addition, it discusses the TCP/IP protocol stack.

Chapter 2: Cloud Security Principles and Frameworks This chapter discusses critical AWS Cloud security concepts such as its shared responsibility model, AWS hypervisors, AWS security certifications, the AWS Well-Architected Framework, and the AWS Marketplace. It also addresses both security *of* the cloud and security *in* the cloud. These concepts are foundational for working with AWS.

Chapter 3: Identity and Access Management This chapter discusses AWS Identity and Access Management (IAM), which sets the foundation for all interactions among the resources in your AWS account. It also covers the different access methods to the AWS IAM services, including AWS Console, AWS command-line tools, AWS software development kits, and the IAM HTTPS application programming interface. Furthermore, the chapter addresses how to protect AWS Cloud environments using multifactor authentication and other best practices.

Chapter 4: Detective Controls This chapter discusses how to gather information about the status of

your resources and the events they produce. It also covers the four stages of the detective controls flow framework: resources state, events collection, events analysis, and action. It also discusses Amazon EventBridge and several AWS Cloud services supporting multiple detective activities.

Chapter 5: Infrastructure Protection This chapter explores AWS networking concepts such as Amazon VPC, subnets, route tables, and other features that are related to network address translation (NAT gateways and NAT instances) and traffic filtering (security groups and network access control lists). It also addresses AWS Elastic Load Balancing and how security services such as AWS Web Application Firewall can provide secure access to your cloud-based applications. Finally, it discusses the AWS Shield and AWS's unique approach to mitigate distributed denial-of-service attacks.

Chapter 6: Data Protection This chapter discusses protecting data using a variety of security services and best practices, including AWS Key Management Service (KMS), the cloud hardware security module (CloudHSM), and AWS Certificate Manager. It also covers creating a customer master key (CMK) in AWS KMS, protecting Amazon S3 buckets, and how Amazon Macie can deploy machine learning to identify personal identifiable information (PII).

Chapter 7: Incident Response This chapter introduces the incident response maturity model's four phases—developing, implementing, monitoring and testing, and updating—and provides best practices for each phase. It also discusses how to react to a range of specific security incidents such as abuse notifications,

insider threats, malware, leaked credentials, and attacks.

Chapter 8: Security Automation This chapter provides an overview of event-driven security and a range of techniques for identifying, responding to, and resolving issues, using tools and techniques such as AWS Lambda, AWS Config, AWS Security Hub, and AWS Systems Manager. It also discusses WAF security automation and isolating bad actors' access to applications.

Chapter 9: Security Troubleshooting in AWS This chapter discusses using AWS CloudTrail, Amazon CloudWatch logs, Amazon CloudWatch events, and Amazon EventBridge to help troubleshoot the operation of AWS Cloud environments. It also presents access control, encryption, networking, and connectivity scenarios that result from common misconfigurations and integration mishandling.

Chapter 10: Creating Your Security Journey in AWS This chapter discusses security in AWS and mapping security controls. It also exemplifies a security journey through three phases: infrastructure protection, security insights and workload protection, and security automation.

Appendix A: Answers to Review Questions This appendix provides the answers to the review questions that appear at the end of each chapter throughout the book.

Appendix B: AWS Security Services Portfolio This appendix provides an overview of the 18 AWS cloud services dedicated to security, identity, and compliance.

Appendix C: DevSecOps in AWS This appendix introduces DevSecOps, the AWS family of services that

implement DevOps practices, and how security controls can be implemented in an automated pipeline.

How to Contact the Publisher

If you believe you've found a mistake in this book, please bring it to our attention. At John Wiley & Sons, we understand how important it is to provide our customers with accurate content, but even with our best efforts an error may occur.

In order to submit your possible errata, please email it to our Customer Service Team at wileysupport@wiley.com with the subject line “Possible Book Errata Submission.”

Interactive Online Learning Environment and Test Bank

Studying the material in the *AWS Certified Security Study Guide: Specialty (SCS-C01) Exam* is an important part of preparing for the AWS Certified Security Specialty (SCS-C01) certification exam, but we provide additional tools to help you prepare. The online test bank will help you understand the types of questions that will appear on the certification exam. The online test bank runs on multiple devices.

Sample Tests The sample tests in the test bank include all the questions at the end of each chapter as well as the questions from the assessment test. In addition, there are two practice exams with 50 questions each. You can use these tests to evaluate your understanding and identify areas that may require additional study.