

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

[Cover](#)

[Title Page](#)

[Table of Exercises](#)

[Introduction](#)

[What Does This Book Cover?](#)

[How to Contact the Publisher](#)

[Interactive Online Learning Environment and Test Bank](#)

[AWS Certified Security Study Guide-Specialty \(SCS-C01\) Exam Objectives](#)

[Objective Map](#)

[Assessment Test](#)

[Answers to Assessment Test](#)

[Chapter 1: Security Fundamentals](#)

[Introduction](#)

[Understanding Security](#)

[Basic Security Concepts](#)

[Foundational Networking Concepts](#)

[Main Classes of Attacks](#)

[Risk Management](#)

[Well-Known Security Frameworks and Models](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

[Chapter 2: Cloud Security Principles and Frameworks](#)

[Introduction](#)

[Cloud Security Principles Overview](#)

[The Shared Responsibility Model](#)

[AWS Compliance Programs](#)

[AWS Well-Architected Framework](#)

[AWS Marketplace](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

[Chapter 3: Identity and Access Management](#)

[Introduction](#)

[IAM Overview](#)

[How AWS IAM Works](#)

[Access Management in Amazon S3](#)

[Identity Federation](#)

[Multi-Account Management with AWS](#)

[Organizations](#)

[Microsoft AD Federation with AWS](#)

[Protecting Credentials with AWS Secrets Manager](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

[Chapter 4: Detective Controls](#)

[Introduction](#)

[Stage 1: Resources State](#)

[Stage 2: Events Collection](#)

[Stage 3: Events Analysis](#)

[Stage 4: Action](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

[Chapter 5: Infrastructure Protection](#)

[Introduction](#)

[AWS Networking Constructs](#)

[Network Address Translation](#)

[Security Groups](#)

[Network Access Control Lists](#)

[Elastic Load Balancing](#)

[VPC Endpoints](#)

[VPC Flow Logs](#)

[AWS Web Application Firewall](#)

[AWS Shield](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

[Chapter 6: Data Protection](#)

[Introduction](#)

[AWS Key Management Service](#)

[Creating a Customer Master Key in AWS KMS](#)

[Understanding the Cloud Hardware Security Module](#)

[AWS Certificate Manager](#)

[Protecting Your S3 Buckets](#)

[Amazon Macie](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

[Chapter 7: Incident Response](#)

[Introduction](#)

[Incident Response Maturity Model](#)

[Incident Response Best Practices](#)

[Reacting to Specific Security Incidents](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

[Chapter 8: Security Automation](#)

[Introduction](#)

[Security Automation Overview](#)

[Event-Driven Security](#)

[Using AWS Lambda for Automated Security Response](#)

[WAF Security Automations](#)

[AWS Config Auto Remediation](#)

[Automating Resolution of Findings Using AWS Security Hub](#)

[Aggregate and Resolve Issues with AWS Systems Manager](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

[Chapter 9: Security Troubleshooting on AWS](#)

[Introduction](#)

[Using Troubleshooting Tools and Resources](#)

[Common Access Control Troubleshooting Scenarios](#)

[Encryption and Decryption Troubleshooting Scenarios](#)

[Network and Connectivity Troubleshooting Scenarios](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

[Chapter 10: Creating Your Security Journey in AWS](#)

[Introduction](#)

[Where to Start?](#)

[Mapping Security Controls](#)

[Security Journey Phased Example](#)

[Summary](#)

[Exam Essentials](#)

[Review Questions](#)

[Appendix A: Answers to Review Questions](#)

[Chapter 1: Security Fundamentals](#)

[Chapter 2: Cloud Security Principles and Frameworks](#)

[Chapter 3: Identity and Access Management](#)

[Chapter 4: Detective Controls](#)

[Chapter 5: Infrastructure Protection](#)

[Chapter 6: Data Protection](#)

[Chapter 7: Incident Response](#)

[Chapter 8: Security Automation](#)

[Chapter 9: Security Troubleshooting on AWS](#)

[Chapter 10: Creating Your Security Journey in AWS](#)

[Appendix B: AWS Security Services Portfolio](#)

[Amazon Cognito](#)

[Amazon Detective](#)

[Amazon GuardDuty](#)

[Amazon Inspector](#)

[Amazon Macie](#)

[AWS Artifact](#)

[AWS Certificate Manager](#)

[AWS CloudHSM](#)

[AWS Directory Service](#)

[AWS Firewall Manager](#)

[AWS Identity and Access Management](#)

[AWS Key Management Service](#)

[AWS Resource Access Manager](#)

[AWS Secrets Manager](#)

[AWS Security Hub](#)

[AWS Shield](#)

[AWS Single Sign-On](#)

[AWS Web Application Firewall](#)

[Appendix C: DevSecOps in AWS](#)

[Introduction](#)

[Dev + Sec + Ops](#)

[AWS Developer Tools](#)

[Creating a CI/CD Using AWS Tools](#)

[Evaluating Security in Agile Development](#)

[Creating the Correct Guardrails Using SAST and DAST](#)

[Security as Code: Creating Guardrails and Implementing Security by Design](#)

[Index](#)

[Copyright](#)

[Acknowledgments](#)

[About the Authors](#)

[About the Technical Editors](#)
[End User License Agreement](#)

List of Tables

Chapter 4

[TABLE 4.1 Comparison of different “views” for configuration items](#)

[TABLE 4.2 AWS CloudTrail: Event types](#)

Chapter 5

[TABLE 5.1 Comparison between NAT gateways and NAT instances](#)

[TABLE 5.2 Security_group rules parameters](#)

[TABLE 5.3 Network ACL rules parameters](#)

Chapter 6

[TABLE 6.1 Symmetric cryptographic encryption algorithms](#)

[TABLE 6.2 Hash algorithms examples](#)

Chapter 8

[TABLE 8.1 Common security use cases covered by AWS Config managed rules](#)

Chapter 9

[TABLE 9.1 Routing table](#)

Chapter 10

[TABLE 10.1 Example matrix mapping current security controls to an AWS environ...](#)

List of Illustrations

Chapter 1

[FIGURE 1.1 Positioning the security_policy](#)

[FIGURE 1.2 The OSI model](#)

[FIGURE 1.3 Comparison between the OSI model and the TCP/IP stack](#)

[FIGURE 1.4 The IPv4 header](#)

[FIGURE 1.5 UDP and TCP headers](#)

[FIGURE 1.6 Contrasting WAF and a web proxy](#)

[FIGURE 1.7 Sample inbound topology](#)

[FIGURE 1.8 Classic topology for VPN termination](#)

[FIGURE 1.9 The security wheel](#)

[FIGURE 1.10 The attack continuum model](#)

[FIGURE 1.11 The attack continuum model applied to malware protection](#)

Chapter 2

[FIGURE 2.1 Services available from the AWS Console](#)

[FIGURE 2.2 Standard Shared Responsibility Model](#)

[FIGURE 2.3 Shared Responsibility Model for container services](#)

[FIGURE 2.4 Shared Responsibility Model for abstracted services](#)

[FIGURE 2.5 AWS Security Documentation](#)

[FIGURE 2.6 AWS Compliance Programs site](#)

[FIGURE 2.7 AWS PCI DSS Anitian Report](#)

[FIGURE 2.8 AWS CSA Compliance site](#)

[FIGURE 2.9 CSA Consensus Assessment site](#)

[FIGURE 2.10 AWS Artifact portal](#)

[FIGURE 2.11 AWS Well-Architected Tool](#)

[FIGURE 2.12 AWS Marketplace Security Solutions](#)

Chapter 3

[FIGURE 3.1 Update Account Settings page](#)

[FIGURE 3.2 IAM users and account permissions](#)

[FIGURE 3.3 Groups and IAM users](#)

[FIGURE 3.4 Resource-based policy example](#)

[FIGURE 3.5 Effective permissions example](#)

[FIGURE 3.6 Identity federation workflow](#)

[FIGURE 3.7 User pool authentication flow](#)

[FIGURE 3.8 Cognito identity pools authentication flow](#)

[FIGURE 3.9 AWS Organizations account hierarchy](#)

[FIGURE 3.10 Authentication workflow using federation between AWS account and...](#)

Chapter 4

[FIGURE 4.1 Detective controls flow framework](#)

[FIGURE 4.2 AWS Config Management console - Configuration Timeline](#)

[FIGURE 4.3 Config history files delivered to an S3 bucket](#)

[FIGURE 4.4 AWS Config and the detective framework](#)

[FIGURE 4.5 AWS CloudTrail digest file object metadata](#)

[FIGURE 4.6 Representation of CloudWatch log events hierarchical grouping](#)

[FIGURE 4.7 Schematic representation of log data for cross-account consumptio...](#)

[FIGURE 4.8 AWS Config Management Console—compliance timeline](#)

[FIGURE 4.9 Amazon Inspector: rules packages, assessment target, and assessme...](#)

[FIGURE 4.10 Sample finding details in Amazon GuardDuty](#)

[FIGURE 4.11 Centralized view in AWS Security Hub grouped by product name](#)

[FIGURE 4.12 AWS Security Hub—insights example](#)

[FIGURE 4.13 SSM automation documents as remediation actions in AWS Config Ru...](#)

[FIGURE 4.14 A generic Amazon EventBridge flow](#)

Chapter 5

[FIGURE 5.1 Amazon VPC dashboard](#)

[FIGURE 5.2 VPC settings](#)

[FIGURE 5.3 VPC1 network topology.](#)

[FIGURE 5.4 Subnet creation](#)

[FIGURE 5.5 Subnet10-AZ1a parameters](#)

[FIGURE 5.6 VPC1 default route table](#)

[FIGURE 5.7 Internet gateway IGW1 creation](#)

[FIGURE 5.8 IGW1 is attached to VPC1.](#)

[FIGURE 5.9 Updated topology.](#)

[FIGURE 5.10 Main route table after IGW1 creation](#)

[FIGURE 5.11 Adding the default route to the main route table](#)

[FIGURE 5.12 Modifying IP Auto-Assignment on Subnet10-AZ1a](#)

[FIGURE 5.13 Two instances deployed on Subnet10-AZ1a](#)

[FIGURE 5.14 The Create NAT Gateway screen](#)

[FIGURE 5.15 NAT gateway creation](#)

[FIGURE 5.16 Route table creation](#)

[FIGURE 5.17 Adding a default route to RouteTable-Subnet20-AZ1b](#)

[FIGURE 5.18 Subnet association](#)

[FIGURE 5.19 Topology with NAT gateway](#)

[FIGURE 5.20 NAT-GW1 CloudWatch statistics](#)

[FIGURE 5.21 Community NAT instances AMIs](#)

[FIGURE 5.22 Security_group SG1](#)

[FIGURE 5.23 Security_groups and an inbound connection](#)

[FIGURE 5.24 SG1 outbound rules](#)

[FIGURE 5.25 VPC1 default security_group](#)

[FIGURE 5.26 EC2-Classic default security_group](#)

[FIGURE 5.27 Default NACL inbound rules](#)

[FIGURE 5.28 Default NACL outbound rules](#)

[FIGURE 5.29 Network topology showing the default NACL](#)

[FIGURE 5.30 Recently created NACL1](#)

[FIGURE 5.31 NACL1 inbound rules](#)

[FIGURE 5.32 NACL1 outbound rules](#)

[FIGURE 5.33 Elastic Load Balancing architecture](#)

[FIGURE 5.34 Select Load Balancer Type screen](#)

[FIGURE 5.35 TG1 basic configuration](#)

[FIGURE 5.36 TG1 registered targets](#)

[FIGURE 5.37 ALB1 Description settings](#)

[FIGURE 5.38 ALB1 Requests Amazon CloudWatch Metric](#)

[FIGURE 5.39 Network topology with ALB1](#)

[FIGURE 5.40 VPC gateway endpoint creation](#)

[FIGURE 5.41 Updated main route table in VPC1](#)

[FIGURE 5.42 VPC interface endpoint creation](#)

[FIGURE 5.43 Flow log creation](#)

[FIGURE 5.44 VPC flow log example](#)

[FIGURE 5.45 WebACL1 creation](#)

[FIGURE 5.46 Adding rules to WebACL1](#)

[FIGURE 5.47 BlockAdminPages custom rule creation](#)

[FIGURE 5.48 WebACL1 Overview graph](#)

Chapter 6

[FIGURE 6.1 Cleartext and ciphertext](#)

[FIGURE 6.2 Asymmetric encryption](#)

[FIGURE 6.3 Signature using an asymmetric algorithm](#)

[FIGURE 6.4 Hash algorithm usage](#)

[FIGURE 6.5 AWS KMS service integration](#)

[FIGURE 6.6 Implementing an end-to-end encryption strategy using AWS KMS](#)

[FIGURE 6.7 Master and data keys](#)

[FIGURE 6.8 KMS master key protection](#)

[FIGURE 6.9 User access methods to the master key](#)

[FIGURE 6.10 Customer master key examples](#)

[FIGURE 6.11 AWS KMS service integration](#)

[FIGURE 6.12 Customer master key details, ARN, alias, KeyID](#)

[FIGURE 6.13 Two roles used to control access to the CMK](#)

[FIGURE 6.14 Role configuration in KMS to control access to the CMK](#)

[FIGURE 6.15 JSON permission policy example diagram](#)

[FIGURE 6.16 JSON permission policy, AWS root account](#)

[FIGURE 6.17 JSON permission policy, IAM user SEC_AWS_BOOK_KMS_ADMIN](#)

[FIGURE 6.18 JSON permission policy, IAM user SEC_AWS_BOOK_KMS_USER](#)

[FIGURE 6.19 Key categories in AWS KMS](#)

[FIGURE 6.20 Allow Key Administrators To Delete This Key option](#)

[FIGURE 6.21 Key Disable and Schedule Key Deletion options](#)

[FIGURE 6.22 Confirm that you want to disable the key.](#)

[FIGURE 6.23 Configuring and checking key rotation](#)

[FIGURE 6.24 CloudHSM configuration](#)

[FIGURE 6.25 CloudHSM configuration validation](#)

[FIGURE 6.26 CloudHSM certificates hierarchy](#)

[FIGURE 6.27 VPC architecture to access ClusterHSM](#)

[FIGURE 6.28 AWS KMS Custom key stores configuration with HSM](#)

[FIGURE 6.29 Custom Key Store KMS integration to CloudHSM](#)

[FIGURE 6.30 ACM integration with AWS-native services scenario](#)

[FIGURE 6.31 ACM private CA scenario](#)

[FIGURE 6.32 Default S3 bucket created as a private bucket](#)

[FIGURE 6.33 Default S3 creation with no encryption](#)

[FIGURE 6.34 SSE-S3 configuration](#)

[FIGURE 6.35 S3 SSE-KMS configuration](#)

[FIGURE 6.36 S3 SSE-KMS with default CMK](#)

[FIGURE 6.37 S3 SSE-KMS with preexisting CMK](#)

[FIGURE 6.38 S3 Replication configuration](#)

[FIGURE 6.39 Key that must be used to decrypt the objects in the S3 origin bu...](#)

[FIGURE 6.40 Destination bucket and the destination encryption key](#)

[FIGURE 6.41 Amazon Macie dashboard](#)

[FIGURE 6.42 Amazon Macie Alerts details console](#)

[FIGURE 6.43 Amazon Macie CloudTrail monitored events](#)

[FIGURE 6.44 Editing Amazon Macie CloudTrail event details](#)

Chapter 7

[FIGURE 7.1 Incident response maturity model](#)

[FIGURE 7.2 AWS Account Security Contact](#)

Chapter 8

[FIGURE 8.1 Security automation logical sequence](#)

[FIGURE 8.2 Amazon S3 events triggering an AWS Lambda function](#)

[FIGURE 8.3 Simple security automation example](#)

[FIGURE 8.4 GuardDuty's TOR Client detection message](#)

[FIGURE 8.5 AWS Lambda environment variable pointing to the Forensics securit...](#)

[FIGURE 8.6 Using Amazon GuardDuty and AWS WAF to automatically block suspici...](#)

[FIGURE 8.7 Reacting to changes detected by AWS CloudTrail](#)

[FIGURE 8.8 WAF Security Automations architecture](#)

[FIGURE 8.9 AWS Config Flow](#)

[FIGURE 8.10 AWS Security Hub as the centerpiece of security automation](#)

[FIGURE 8.11 AWS IAM Access Analyzer: creating an analyzer](#)

[FIGURE 8.12 Creating an Amazon CloudWatch rule for the custom action](#)

[FIGURE 8.13 Creating the bucket without Block Public Access](#)

[FIGURE 8.14 Finding from IAM Access Analyzer on the AwsS3Bucket resource](#)

[FIGURE 8.15 Automated Amazon S3 bucket closure from AWS Security Hub](#)

[FIGURE 8.16 Block All Public Access enabled](#)

Chapter 9

[FIGURE 9.1 Effective permissions example](#)

[FIGURE 9.2 Architecture of a NAT gateway](#)

[FIGURE 9.3 Architecture of an Internet gateway](#)

[FIGURE 9.4 Peering example](#)

[FIGURE 9.5 No transitivity example](#)

Appendix B

[FIGURE B.1 Amazon Cognito icon](#)

[FIGURE B.2 Amazon Detective icon](#)

[FIGURE B.3 Amazon GuardDuty icon](#)

[FIGURE B.4 Amazon Inspector icon](#)

[FIGURE B.5 Amazon Macie icon](#)

[FIGURE B.6 AWS Artifact icon](#)

[FIGURE B.7 AWS Certificate Manager icon](#)

[FIGURE B.8 AWS CloudHSM icon](#)

[FIGURE B.9 AWS Directory Service icon](#)

[FIGURE B.10 AWS Firewall Manager icon](#)

[FIGURE B.11 AWS Identity and Access Management icon](#)

[FIGURE B.12 AWS Key Management Service icon](#)

[FIGURE B.13 AWS Resource Access Manager icon](#)

[FIGURE B.14 AWS Secrets Manager icon](#)

[FIGURE B.15 AWS Security Hub icon](#)

[FIGURE B.16 AWS Shield icon](#)

[FIGURE B.17 AWS Single Sign-On](#)

[FIGURE B.18 AWS Web Application icon](#)

Appendix C

[FIGURE C.1 Continuous delivery vs. continuous deployment](#)

[FIGURE C.2 Steps of software release process](#)

[FIGURE C.3 AWS X-Ray service map](#)

[FIGURE C.4 AWS X-Ray Traces](#)

[FIGURE C.5 Amazon CloudWatch panel](#)

[FIGURE C.6 The repository you created in the AWS Console](#)

[FIGURE C.7 Committed source code](#)

[FIGURE C.8 Role configuration](#)

[FIGURE C.9 Project configuration](#)

[FIGURE C.10 Source screen](#)

[FIGURE C.11 Environment screen](#)

[FIGURE C.12 Buildspec screen](#)

[FIGURE C.13 Artifacts screen](#)

[FIGURE C.14 Logs screen](#)

[FIGURE C.15 Pipeline settings](#)

[FIGURE C.16 Add Source Stage screen](#)

[FIGURE C.17 Add Build Stage screen](#)

[FIGURE C.18 Add Deploy Stage screen](#)

[FIGURE C.19 Pipeline result](#)

[FIGURE C.20 Pipeline with failed status](#)

[FIGURE C.21 Pipeline with Success status](#)

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**



Table of Exercises

<u>Exercise 2.1</u>	<u>Generating the PCI DSS Report in the AWS Artifact Portal</u>
<u>Exercise 2.2</u>	<u>Checking the ISO 27001 and ISO 27017 Reports</u>
<u>Exercise 2.3</u>	<u>Using the Well-Architected Tool</u>
<u>Exercise 3.1</u>	<u>Change the Root Account Password</u>
<u>Exercise 3.2</u>	<u>Enable Multifactor Authentication for the Root Account</u>
<u>Exercise 3.3</u>	<u>Create an IAM User with Administrator Access Permissions</u>
<u>Exercise 3.4</u>	<u>Create an IAM Group with Amazon S3 Read-Only Access Role</u>
<u>Exercise 3.5</u>	<u>Create an Amazon S3 Bucket</u>
<u>Exercise 3.6</u>	<u>Add a User to the AmazonS3Viewers Group</u>
<u>Exercise 3.7</u>	<u>Force SSL Encryption for an Amazon S3 Bucket</u>
<u>Exercise 4.1</u>	<u>Set Up AWS Config</u>
<u>Exercise 4.2</u>	<u>Set Up a Trail in CloudTrail</u>
<u>Exercise 4.3</u>	<u>AWS CloudTrail Integration with Amazon CloudWatch Logs</u>
<u>Exercise 4.4</u>	<u>Create an Amazon CloudWatch Alarm</u>
<u>Exercise 4.5</u>	<u>AWS Config Rules</u>
<u>Exercise 4.6</u>	<u>Enable Amazon GuardDuty in Your Account</u>
<u>Exercise 4.7</u>	<u>Enable AWS Security Hub in Your Account</u>
<u>Exercise 4.8</u>	<u>AWS Config Rules Remediation</u>

- [**Exercise 4.9**](#) [AWS CloudTrail Integration with Amazon EventBridge](#)
- [**Exercise 5.1**](#) [Create a VPC and Subnets](#)
- [**Exercise 5.2**](#) [Create an Internet Gateway](#)
- [**Exercise 5.3**](#) [Create NAT Gateways](#)
- [**Exercise 5.4**](#) [Create Security Groups](#)
- [**Exercise 5.5**](#) [Create an NACL](#)
- [**Exercise 5.6**](#) [Elastic Load Balancing](#)
- [**Exercise 5.7**](#) [Work with VPC Endpoints](#)
- [**Exercise 5.8**](#) [Checking VPC Flow Logs](#)
- [**Exercise 5.9**](#) [Create and Test an AWS Web Application Firewall](#)
- [**Exercise 6.1**](#) [Create a KMS Key](#)
- [**Exercise 6.2**](#) [Create an S3 Bucket and Use a KMS Key to Protect the Bucket](#)
- [**Exercise 6.3**](#) [Protecting RDS with KMS](#)
- [**Exercise 6.4**](#) [Protecting EBS with KMS](#)
- [**Exercise 6.5**](#) [Protect Your S3 Buckets with Block Public Access Settings and SCP](#)
- [**Exercise 6.6**](#) [Replicate Encrypted S3 Objects across Regions](#)
- [**Exercise 6.7**](#) [Protect Your S3 Buckets with a Resource Policy and VPC Endpoints](#)
- [**Exercise 7.1**](#) [Automatically Create a Table for Querying AWS CloudTrail Logs with Amazon Athena](#)
- [**Exercise 7.2**](#) [Manually Create a Table for Querying AWS CloudTrail Logs with Amazon Athena](#)
- [**Exercise 7.3**](#) [Query AWS CloudTrail Logs with Amazon Athena](#)
- [**Exercise 7.4**](#) [Rotate AWS IAM Credentials](#)

- Exercise 8.1** [Isolate Instances Using a TOR Anonymization Network](#)
- Exercise 8.2** [Implement WAF Security Automations](#)
- Exercise 8.3** [Automatically Configure All Buckets to Default to AES256 for Server-Side Encryption](#)
- Exercise 8.4** [Automatically Remove All SSH Access Open to the World](#)
- Exercise 9.1** [Creating a Trail in AWS CloudTrail](#)
- Exercise 9.2** [Creating an Internet Gateway](#)
- Exercise 9.3** [Creating a Peering Connection](#)
- Exercise 9.4** [Creating a VPC Flow Log](#)
- Exercise 9.5** [Removing a VPC Flow Log](#)

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.