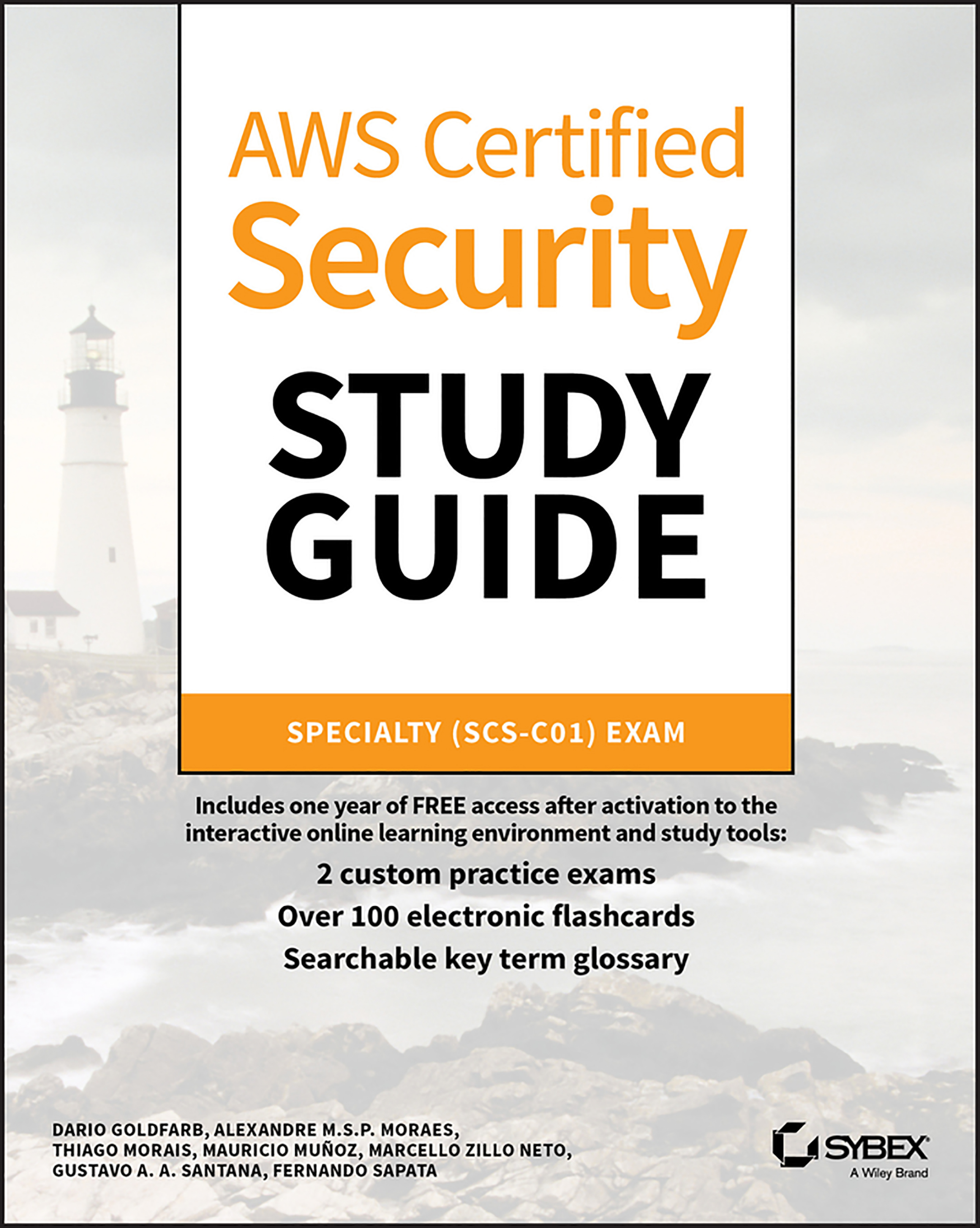

AWS Certified Security STUDY GUIDE

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

AWS Certified Security

Study Guide

Specialty (SCS-C01) Exam

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

Published simultaneously in Canada and the United Kingdom

ISBN: 978-1-119-65881-8
ISBN: 978-1-119-65883-2 (ebk.)
ISBN: 978-1-119-65884-9 (ebk.)

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or Web site may provide or recommendations it may make. Further, readers should be aware that Internet Web sites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services or to obtain technical support, please contact our Customer Care Department within the U.S. at (877) 762-2974, outside the U.S. at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2020950308

Acknowledgments

First and foremost, we offer our most profound thanks to our spouses, children, and families, whose support and understanding during our many long hours of writing and reviews gave us the time and strength to create this book. This book would not have been possible without our wonderful families.

We would also like to show our appreciation for Amazon Web Services (AWS) for providing cloud-computing platforms, APIs, and the Specialty (SCS-C01) Exam to the world at large. We are excited to be an active part of this transformative growth and development of secure cloud computing in the world today.

We'd also like to thank associate publisher Jim Minatel and acquisitions editor Ken Brown for entrusting us with the role of creating this study guide for Wiley. We also appreciate the insights of technical editors Daniel Garcia and Todd Montgomery, whose attention to detail elevated this book to the next level. Thanks also goes to project editor Kelly Talbot, production editor Barath Kumar Rajasekaran, copy editor Liz Welch, and the entire team at Wiley for their guidance and assistance in making this book. We'd also like to thank all of our colleagues and experts who consulted with us while we were writing this book—too many to name here, but we are grateful for your suggestions and contributions.

And perhaps more than anyone else, we would like to thank our readers. We are grateful for the trust that you have placed in us to help you study for the exam, and we have worked hard to prepare you for your journey.

—The Authors

About the Authors

Dario Goldfarb is a security solutions architect at Amazon Web Services in Latin America with more than 15 years of experience in cybersecurity, helping organizations from different industries to improve their cyber-resiliency. Dario enjoys sharing security knowledge through speaking at public events, presenting webinars, teaching classes for universities, and writing blogs and articles for the press. He has a significant number of certifications, including CISSP, the Open Group Master IT Architect, and the AWS Security Specialty certification, and holds a degree in systems engineering from UTN (Argentina) and a diploma on cybersecurity management from UCEMA (Argentina).

Alexandre M. S. P. Moraes, CCIE No. 6063, worked as a systems engineer and consulting systems engineer for Cisco Brazil from 1998 to 2014, in projects involving not only security and VPN technologies but also routing protocol and campus design, IP multicast routing, and MPLS networks design. He is the author of *Cisco Firewalls* (Cisco Press, 2011) and has delivered many technical sessions related to security in market events such as Cisco Networkers and Cisco Live (Brazil, United States, United Kingdom). In 2014, Alexandre started a new journey as a director for Teltec Solutions, a Brazilian systems integrator that is highly specialized in the fields of network design, security architectures, and cloud computing. Alexandre holds the CISSP, the CCSP, and three CCIE certifications (routing/switching, security, and service provider). He graduated in electronic engineering from the Instituto Tecnológico de Aeronáutica (ITA–Brazil) and holds a master's degree in mathematics (group theory) from Universidade de Brasília (UnB–Brazil).

Thiago Morais is the leader of solutions architecture teams at Amazon Web Services in Brazil. With more than 20 years of experience in the IT industry, he has worked at startups, advertising agencies, and information security companies, developing and implementing solutions for various industries. In recent years, Thiago has been focused on cloud computing and has specialized in serverless architectures, leading a team that works with large startups and software vendors to help them build solutions in the cloud. He currently holds five AWS certifications and is a regular speaker at local and global technology conferences. Thiago holds a degree in computer science from Universidade Ibirapuera (UNIB–Brazil) and an MBA degree from Insper (Brazil).

Mauricio Muñoz is senior manager of a specialist solutions architects team at Amazon Web Services in Latin America. Mauricio started more than 20 years ago working in information security and has been CISSP certified since 2005. Throughout his career, Mauricio has extended his field of expertise by working on projects for enterprise customers in areas such as networking, application integration, analytics, and cloud computing. Passionate about learning and sharing knowledge, Mauricio was an authorized instructor for CISSP and CEH certification training, as well as for other related technical certifications (including more recently AWS training on the delivery of architecting). He is a frequent speaker for both cloud computing and industry events in Latin America. Currently, Mauricio holds seven

AWS certifications. Mauricio has developed his professional career in different countries around Latin America, holding the title of electronics engineer from Pontificia Universidad Javeriana (PUJ–Colombia) and executive MBA from Insper (Brazil).

Marcello Zillo Neto is a chief security advisor and former chief information security officer (CISO) in Latin America. He has over 20 years of experience in information security, network security, cybersecurity, risk management, and incident response, helping banks, service providers, retail customers, and many other verticals to create their security journey to the cloud. Marcello is a frequent speaker at cloud computing and security events and holds a degree in computer engineering from Universidade São Francisco (USF), an executive MBA from Insper (Brazil), and executive training in digital business strategy and machine learning at MIT. He is also a professor, teaching information security, cloud security, incident response, and security strategy, among other cybersecurity disciplines in universities in Brazil such as Fundação Instituto de Administração (FIA). He also has the following certifications: Certified Information Systems Security Professional (CISSP), AWS Certified Solutions Architect, AWS Certified Security Specialist, and Lead Auditor–ISO 27001.

Gustavo A. A. Santana is the leader of the specialist and telecommunications solutions architecture teams at Amazon Web Services in Latin America. With more than 20 years of experience in the IT industry, Gustavo has worked on multiple enterprise and service provider data center projects that required extensive integration across multiple technology areas such as networking, application optimization, storage, servers, end-to-end virtualization, automation, and cloud computing. A true believer in education as a technology catalyst, he has also dedicated himself to the technical development of IT professionals from multiple customers, partners, and vendors. A frequent speaker at cloud computing and data center industry events, Gustavo holds a degree in computer engineering from Instituto Tecnológico de Aeronáutica (ITA–Brazil), an MBA in strategic IT management from Fundação Getúlio Vargas (FGV–Brazil), six AWS certifications, VMware Certified Implementation Expert in Network Virtualization (VCIX-NV), and three Cisco Certified Internetwork Expert (routing/switching, storage networking, and data center) certifications. He is also the author of three books: *Data Center Virtualization Fundamentals* (Cisco Press, 2013), *CCNA Cloud CLD-FND 210-451 Official Cert Guide* (Cisco Press, 2016), and *VMware NSX Network Virtualization Fundamentals* (VMware Press, 2018).

Fernando Sapata is a principal business development manager for serverless at Amazon Web Services in Latin America. Fernando started developing software in Clipper Summer 87 at 13 years old, and today he has more than 19 years of experience in the IT industry. Fernando has worked with multiple segments such as Internet service providers, telecommunications, consulting services, storage, and now, cloud computing. With solid experience in software development and solutions architecture, Fernando worked as a principal solutions architect at AWS for four years, helping customers in their cloud journey. He is an active member of serverless advocacy, frequently speaking in cloud computing and community events worldwide. He is a teacher, writer, podcaster, and a believer that knowledge and technology can transform lives.

About the Technical Editors

Daniel Garcia is a principal security SA in Amazon Web Services, currently holds six AWS certifications, and has more than 20 years of experience in networking, network security, and cybersecurity. During his career, he has helped companies in multiple verticals such as telecom, banking, insurance, retail, oil and gas, government, and education, among others, to successfully craft and implement their networking and cybersecurity strategies, always striving to design efficient architectures to protect, detect, and respond. Daniel holds an electrical engineering degree from Universidade de São Paulo (USP–Brazil), and a master's degree in business administration from Fundação Getúlio Vargas (FGV–Brazil).

Todd Montgomery is a senior data center networking engineer for a large international consulting company, where he is involved in network design, security, and implementation of emerging data center and cloud-based technologies. He holds six AWS certifications, including the Big Data specialty certification. Todd holds a degree in electronics engineering, as well as multiple certifications from Cisco Systems, Juniper Networks, and CompTIA. Todd also leads the AWS certification meetup group in Austin, Texas.

Contents at a Glance

Contents

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.

Flashcards The flashcards in the test bank will push the limits of what you should know for the certification exam. There are 100 questions that are provided in digital format. Each flashcard has one question and one correct answer.

Glossary The online glossary is a searchable list of key terms introduced in this exam guide that you should know for the AWS Certified Security Specialty (SCS-C01) certification exam.

NOTE

Go to www.wiley.com/go/sybextestprep to register and gain access to this interactive online learning environment and test bank with study tools.

To start using these tools to study for the AWS Certified Security Specialty (SCS-C01) exam, go to www.wiley.com/go/sybextestprep, register your book to receive your unique PIN, then once you have the PIN, return to www.wiley.com/go/sybextestprep, find your book and click register or login and follow the link to register a new account or add this book to an existing account.

AWS Certified Security Study Guide–Specialty (SCS-C01) Exam Objectives

This table shows the extent, by percentage, of each domain represented on the actual examination.

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%

NOTE

Exam objectives are subject to change at any time without prior notice and at AWS's sole discretion. Please visit the AWS Certified Security–Specialty website (aws.amazon.com/certification/certified-security-specialty) for the most current listing of exam objectives.

Objective Map

Objective	Chapter
Domain 1: Incident Response	
1.1 Given an AWS abuse notice, evaluate the suspected compromised instance or exposed access keys	7

Objective	Chapter
1.2 Verify that the Incident Response plan includes relevant AWS services	1, 2, 7, 10
1.3 Evaluate the configuration of automated alerting, and execute possible remediation of security-related incidents and emerging issues	8, 10
Domain 2: Logging and Monitoring	
2.1 Design and implement security monitoring and alerting	1, 4, 10
2.2 Troubleshoot security monitoring and alerting	9
2.3 Design and implement a logging solution	4, 10
2.4 Troubleshoot logging solutions	9
Domain 3: Infrastructure Security	
3.1 Design edge security on AWS	1, 5, 8, 10
3.2 Design and implement a secure network infrastructure	1, 5, 10
3.3 Troubleshoot a secure network infrastructure	5, 9
3.4 Design and implement host-based security	2, 4, 10
Domain 4: Identity and Access Management	
4.1 Design and implement a scalable authorization and authentication system to access AWS resources	1, 3, 10
4.2 Troubleshoot an authorization and authentication system to access AWS resources	3, 9
Domain 5: Data Protection	
5.1 Design and implement key management and use	6, 10
5.2 Troubleshoot key management	6, 9
5.3 Design and implement a data encryption solution for data at rest and data in transit	1, 6, 10

Assessment Test

1. Which one of the following components should not influence an organization's security policy?

   A. Business objectives

   B. Regulatory requirements

   C. Risk

   D. Cost–benefit analysis

   E. Current firewall limitations

2. Consider the following statements about the AAA architecture:

   I. Authentication deals with the question "Who is the user?"

   II. Authorization addresses the question "What is the user allowed to do?"

   III. Accountability answers the question "What did the user do?"

   Which of the following is correct?

   A. Only I is correct.

   B. Only II is correct.

   C. I, II, and III are correct.

   D. I and II are correct.

   E. II and III are correct.

3. What is the difference between denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks?

   A. DDoS attacks have many targets, whereas DoS attacks have only one each.

   B. DDoS attacks target multiple networks, whereas DoS attacks target a single network.

   C. DDoS attacks have many sources, whereas DoS attacks have only one each.

   D. DDoS attacks target multiple layers of the OSI model and DoS attacks only one.

   E. DDoS attacks are synonymous with DoS attacks.

4. Which of the following options is incorrect?

   A. A firewall is a security system aimed at isolating specific areas of the network and delimiting domains of trust.

   B. Generally speaking, the web application firewall (WAF) is a specialized security element that acts as a full-reverse proxy, protecting applications that are accessed through HTTP.

   C. Whereas intrusion prevention system (IPS) devices handle only copies of the packets and are mainly concerned with monitoring and alerting tasks, intrusion detection system (IDS) solutions are deployed inline in the traffic flow and have the inherent design goal of avoiding actual damage to systems.