AWS Certified Security - Specialty Certification Guide (SCS-C01)

AWS security concepts and best practices

Nikhil Agarwal

www.bpbonline.com

First Edition 2024

ISBN: 978-93-55516-640

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true to correct and the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

Dedicated to

My parents, the original programmers of my life; my wife, the ultimate debugger of my dreams and my friends, the trusted network

About the Author

Nikhil is an innovator in the field of cyber security, recognized by his remarkable knowledge and innovative approach. When it comes to data and cloud security, he is the go-to guy. He leads large-scale projects, helping clients solve their most pressing data security and cloud security challenges.

Nikhil's reputation as a noted technology expert is well-deserved, as he is passionate about sharing his knowledge and building communities. He has also co-founded an open-source emerging tech community in India called FutureGPT.

In recognition of his outstanding contributions to the field, Nikhil was ranked 18th globally in Cyber Security, 10th in Emerging Technologies, and 3rd in Cloud Security Leaders by Onalytica in 2021. His accomplishments were further celebrated in 2022 when he was named a Cloud Security Champion by the Cloud Security Alliance and recently awarded Cyber Security Champion in 2024 by Bsides.

He has a proven ability to work across cultures and serve clients globally, having previously held senior leadership roles with Fortanix Inc, Deloitte Singapore, PwC Thailand, Quick Heal, and Atos.

About the Reviewer

Ritesh Gohil is a dedicated Information Security Engineer with over five years of professional experience in Cyber Security and Penetration Testing. His expertise spans across Web applications, APIs, Mobile (Android and iOS) applications, and Cloud Security / Penetration Testing. He has made significant contributions to the field by publishing eight CVEs in Mitre and is recognized as one of the top 25 researchers on the Yogosha platform. Ritesh has also received multiple honorable mentions from Google and Apple.

Ritesh specializes in advanced AWS security solutions, ensuring robust protection for cloud environments, and maintaining compliance standards. His passion for cybersecurity is evident through his participation in bug bounties and his active involvement in security research, where he has reported numerous vulnerabilities and received commendations from the Indian Government for his responsible vulnerability disclosure.

He is currently working at Ryanair, Europe's Favourite Airline, where he is part of the Red Team, responsible for penetration testing, security audits, and fortifying digital infrastructure. Ritesh holds multiple industry certifications, including AWS Certified Security – Specialty, eWPTXv2, eCPPTv2, CRTP, eJPT, and CEH. He completed his MSc in Cyber Security from the National College of Ireland. His dedication to the field is further demonstrated through his active participation in security conferences and contributions to various security platforms.

Acknowledgement

Creating this book has been an incredible journey, and I could not have done it without the amazing support of so many wonderful people.

First, to my parents: thank you for your endless love and support. Your constant encouragement and belief in me have been my foundation.

To my wonderful wife: thank you for your patience, understanding, and constant support. Your love and encouragement have been my greatest source of motivation.

To my friends: thank you for your kindness, laughter, and always being there when I needed a break. Your support has made every challenge seem manageable.

Finally, to everyone who has been a part of this journey, whether directly or indirectly: your contributions, no matter how small, have made a significant impact. Thank you for being a part of this adventure.

This book is a testament to the power of support, collaboration, and the collective effort of many wonderful people. Thank you all for being a part of my life and this journey.

Preface

Welcome to the **AWS Certified Security - Specialty Certification Guide (SCS-C01)**, an exhaustive guide that is specifically designed to assist you in managing the complexities of AWS security and achieving this highly valued certification. This book has been designed to ensure that you have a comprehensive understanding of the essential concepts, practices, and technologies necessary to secure AWS environments.

Chapter 1: Getting Started with Foundations of Cloud Security- This chapter covers the foundation for your learning experience by addressing the fundamental principles of cloud security. You will gain an understanding of the different security challenges and benefits that cloud computing offers.

Chapter 2: The AWS Certified Security-specialty Exam Domains - This chapter covers the specific domains that are covered by the certification exam. In order to ensure that you have sufficient preparation for every section of the exam, this chapter outlines the key areas of interest that you need to focus on.

Chapter 3: Identity and Access Management: Laying a Solid Foundation - This chapter covers the fundamentals of IAM. To ensure that access to your AWS resources is both secure and effective, you will learn how to manage users, groups, roles, and permissions.

Chapter 4: Securing Infrastructure Design in AWS - This chapter covers the best practices for designing secure AWS infrastructure. It also covers methods for securing your digital assets and network from a variety of threats.

Chapter 5: Securing Network Design in AWS - This chapter covers the specifics of securing your network architecture. You will learn about VPCs, subnets, security groups, and other network elements that are essential to the security of AWS.

Chapter 6: Application and Host-based Security - This chapter covers the applications and host environments. Best practices for protecting your code, applications, and operating systems are also discussed in this chapter.

Chapter 7: Data-at-rest, Data-in-transit and Data-in-use Protection - This chapter covers data security in Cloud. To ensure the security of your sensitive information, you will learn about a variety of data security measures, such as encryption, access controls, and data obfuscation.

Chapter 8: Encryption and Key Management - This chapter covers the field of encryption and Key Management. This chapter provides a comprehensive explanation of the methods and services necessary to effectively implement and perform encryption and key management within AWS.

Chapter 9: AWS Multi-account Architecture and Access Control - This chapter covers the benefits and complexities of managing multiple AWS accounts. You'll learn how to establish a secure multi-account strategy that ensures proper access control and governance.

Chapter 10: Infrastructure-as-Code and CI/CD - This chapter covers the modern practices for automating infrastructure deployment and management. You will learn how to use Infrastructure-as-Code (IaC) tools and continuous integration/continuous deployment (CI/CD) pipelines to maintain secure and compliant environments.

Chapter 11: Application and Network Logging Strategies - This chapter covers how to promptly detect and respond to security incidents by implementing effective logging strategies.

Chapter 12: Troubleshooting Security and Monitoring Alerts - This chapter covers the practical approaches to troubleshooting security issues and responding to monitoring alerts. The tools necessary to maintain a secure and resilient AWS environment are discussed in this chapter.

Chapter 13: Incident Detection, Response, and Remediation - This chapter covers the critical aspects of incident management. To reduce the impact of security incidents on your organization, you will learn how to detect, respond to, and resolve them.

Chapter 14: Compliance, Governance, and Data Security Standards - This chapter covers the essential requirements for maintaining compliance with various standards and regulations. You will gain knowledge about establishing governance frameworks and adhering to data security standards in this course.

Chapter 15: Assessment, Audit, and Evidence Collection - This chapter covers the guidance on conducting security assessments and audits. In order to effectively gather and present evidence of your security practices, this chapter ensures that you are prepared.

Chapter 16: Automated Security Investigation and Remediation - This chaptercovers the implementation of automation in security operations. You will learn how to use AWS services to automate security investigations and remediation duties, which will improve your capacity to respond to threats promptly.

Chapter 17: Exam Preparation Tips - This chapter covers the conclusion of the book by summarizing the primary topics and offering concluding insights on your progress to the role of AWS Security Specialist.

Whether you are new to AWS or seeking to expand your knowledge, this book is designed for developers and security professionals. This guide will help you gain the skills and confidence to excel in the field of AWS security and achieve your certification objectives. This book will be both informative and beneficial.

Coloured Images

Please follow the link to download the
Coloured Images of the book:

https://rebrand.ly/mdp9klg

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1

Getting Started with Foundations of Cloud Security

Introduction

Computing in the cloud has evolved as a crucial technological advancement that has significantly altered the method in which we manage, process, and store data. The traditional approach to computing has been fundamentally altered as a result of the provision of an infrastructure that is both scalable and adaptable and that can be accessed at any time and from any location. On the other hand, with tremendous power comes great responsibility, and the obligation of safeguarding the cloud infrastructure falls on both the **Cloud Service Providers** (**CSPs**) and the clients who use their services. The principles of cloud security, the shared responsibility paradigm, risk assessment, threat modeling, and best practices are going to be covered in this chapter.

Structure

This chapter will cover the following topics:

- Understanding the fundamentals of cloud security
- Overview of the shared responsibility model
- Risk assessment and threat modeling
- Cloud security recommended practices

Objectives

This introduction chapter will offer readers with a basic grasp of the fundamentals of cloud security and will build the basis for the rest of the book, which will delve into particular tools and approaches for securing cloud environments. The goal of this chapter is to provide readers with a solid understanding of the fundamentals of cloud security. The reader will obtain a clear grasp of the significance of cloud security as well as how to approach it methodically after going through an overview of the shared responsibility model, risk assessment, and threat modeling. In addition to that, this chapter will present readers with a set of best practices that they should follow to keep their cloud environments safe.

Understanding the fundamentals of cloud security

Data, apps, and the underlying infrastructure in a cloud computing environment all need to be protected for cloud security to be effective. Access control, encryption, network security, **Identity and Access Management** (**IAM**), and disaster recovery are some of the different security methods that are included in this. It is essential to have a solid understanding of the principles of cloud security to guarantee the safety of cloud-based infrastructure. The following are some of the central ideas:

- **Confidentiality:** The protection of sensitive information from being accessed or disclosed in an unapproved manner is what is meant by the term confidentiality.
- **Integrity:** It refers to the protection of data from unintended changes or deletions made by unauthorized parties.
- **Availability:** This refers to the guarantee that the data and services will be accessible whenever they are needed.
- **Authentication:** This refers to the process of determining if a user or a computer system is who they claim to be.
- **Authorization:** This refers to the process of allowing access to resources according to user roles and permissions. This procedure is referred to as "authorization."
- **Non-repudiation:** This is the assurance that a user cannot deny doing an action; it is also known as the non-repudiation guarantee.

Overview of the shared responsibility model

The shared responsibility model is a framework that defines the responsibilities of both the **Cloud Service Provider** (**CSP**) and the client about the protection of the cloud's underlying infrastructure. The model shifts based on the deployment model for the cloud, which can be either public, private, or hybrid. Refer to the following *Figure 1.1*, showing the shared responsibility model for a CSP:

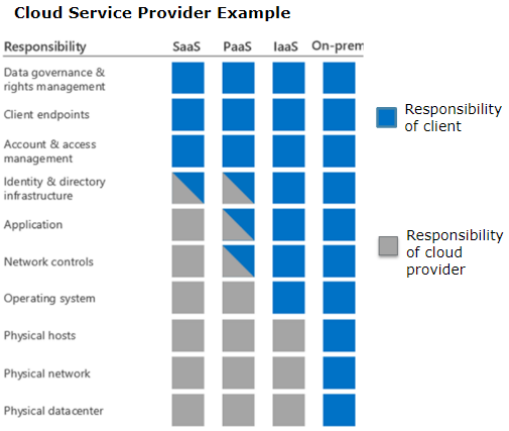

Figure 1.1: *Shared Responsibility Model for a CSP*

The cloud service provider is responsible for the security of the underlying infrastructure in the public cloud deployment paradigm, whereas the client is responsible for the security of the applications and data. The customer is responsible for the security of the underlying infrastructure when the private cloud deployment model is used, while the cloud service provider is responsible for the security of the applications and data. The customer and the CSP both bear equal responsibility for the safety of the infrastructure, apps, and data when it comes to hybrid cloud deployment models. Because it guarantees that all parties involved are aware of their obligations and take appropriate actions to safeguard the cloud infrastructure, the shared responsibility model is an essential component of cloud security.

Note: Ownership of risks, controls, and outcomes are underpinned by a shared responsibility matrix. Risk management responsibilities can vary sharply depending on the selected cloud deployment and service models. Hence it is critical to understand the areas of responsibility within this model, which allows us to define the scope of the assessment.

Risk assessment and threat modeling

The two most important parts of cloud security are risk assessment and threat modeling. Risk assessment is the process of finding possible risks and weaknesses in the cloud system and figuring out how likely it is that a threat will use them. Threat modeling is the process of looking at possible risks and how they might affect the cloud system. By doing a risk assessment and threat modeling, enterprises can find possible security holes and fix them by putting in place the right security controls.

When looking at the security of a cloud service provider from a technical point of view, risk assessment and threat modeling are very important steps. These practices help find possible risks, weaknesses, and threats to the infrastructure, data, and services of the provider.

Here is what you need to know about risk assessment and threat modeling for CSP:

- **Risk assessment:** Risk assessment is the process of finding, analyzing, and rating possible risks related to the technical infrastructure and activities of the cloud service provider. Its goal is to figure out how likely and bad different risks are so that prevention efforts can be prioritized. Usually, the following steps make up the process:
- **Asset identification:** Determine which servers, databases, apps, and sensitive data are part of the cloud service's asset pool.
- **Risk identification:** Look for possible risks and threats that could hurt the cloud service's privacy, security, or ability to be used. This can include risks like unauthorized entry, data leaks, system failures, and threats from inside the organization.
- **Risk analysis:** Analyse the risks you've found to find out what they might mean, how likely they are to happen, and what might happen as a result. This research helps prioritize risks so that more steps can be taken to reduce them.
- **Risk evaluation:** Evaluate the risks you have found based on how bad they are and put them in order of how important they are to fix. This step looks at how the change might affect the cloud service provider, its customers, and the data they store.

How cloud security works with shared responsibility

The shared responsibility model is a system that shows how a CSP and its customer should handle security. It is like renting an apartment, the landlord takes care of the building, but you are responsible for keeping your area tidy and safe.

The security of the underlying cloud infrastructure is the responsibility of the **Cloud Service Provider** (**CSP**). The physical security of the data centers is also taken care of by them.

The customer is in charge of securing the data and apps they store or use in the cloud. This includes securing their gadgets used to access the cloud, data encryption, and user access control.

A quick look at cloud computing model

Different models for cloud computing offer different amounts of service and responsibility:

- **Infrastructure as a Service (IaaS):** You rent everything you need to build something, like computers, storage, and networking. In terms of security and configuration, you have the most control but also the most responsibility. It's kind of like renting a simple office.