AWS Certified Security – Specialty Exam Guide

Build your cloud security knowledge and expertise as an AWS Certified Security Specialist (SCS-C01)

Stuart Scott

Packt
www.packt.com

AWS Certified Security – Specialty Exam Guide

Build your cloud security knowledge and expertise as an AWS Certified Security Specialist (SCS-C01)

Stuart Scott

Packt

BIRMINGHAM - MUMBAI

Packt.com

Subscribe to our online digital library for full access to over 7,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Improve your learning with Skill Plans built especially for you
- Get a free eBook or video every month
- Fully searchable for easy access to vital information
- Copy and paste, print, and bookmark content

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.packt.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at customercare@packtpub.com for more details.

At www.packt.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

AWS Certified Security – Specialty Exam Guide

Commissioning Editor: Vijin Boricha
Acquisition Editor: Meeta Rajani
Content Development Editor: Carlton Borges
Senior Editor: Rahul Dsouza
Technical Editor: Sarvesh Jaywant
Copy Editor: Safis Editing
Project Coordinator: Neil Dmello
Proofreader: Safis Editing
Indexer: Rekha Nair
Production Designer: Joshua Misquitta

First published: August 2020

Production reference: 1040820

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-78953-447-4

www.packt.com

Contributors

About the author

With over two decades in the IT industry, **Stuart Scott** has an extensive background covering a range of technologies, but his passion is centered around **Amazon Web Services** (**AWS**).

Stuart is the AWS content and security lead at Cloud Academy where he has created over 80 courses teaching over 100,000 students. His content focuses on cloud security and compliance, and how to implement and configure AWS services to protect, monitor, and secure customer data in AWS.

Stuart has written many cloud security blogs and regularly hosts webinars with AWS and leading AWS partners.

He is a certified expert within the Experts-Exchange community. In January 2016 he was awarded 'Expert of the Year' for his sharing of knowledge on cloud services with the community.

A huge thank you to my family for their continued support throughout this book, in particular, my loving wife Lisa!

Also, to my mum and dad, who have always encouraged me to do my best to achieve my goals – thank you for everything!

About the reviewer

Sriya Potham is an experienced security professional and cloud evangelist and is currently a cloud security architect managing e-commerce, AWS, and SaaS security. She has obtained both the AWS Solutions Architect – Associate and AWS Security – Specialty certifications and has been involved in the development of cloud programs at major Fortune 500 companies in the travel, financial, and consumer goods sectors. Outside of work, she enjoys practicing and teaching yoga.

I'd like to thank my family and friends for their part in helping me grow and learn every day.

Packt is searching for authors like you

If you're interested in becoming an author for Packt, please visit `authors.packtpub.com` and apply today. We have worked with thousands of developers and tech professionals, just like you, to help them share their insight 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.

Table of Contents

Section 3: Security - a Layered Approach

Preface

This book will provide you with a deep understanding of the different security mechanisms that can be applied when architecting within the cloud, specifically within AWS. Security should always be the number one factor when deploying solutions, and understanding the impact of security at every layer is a requirement for any security practitioner.

You will be guided through every layer of AWS security from the following perspectives:

- Access management and the different techniques that can be applied to enforce it
- Policy management to understand how to define permissions that should be applied
- Host security, defining best practices on protecting instances
- Network and application security, ensuring neither are left vulnerable to exposures, vulnerabilities, or attacks
- Incident response, and how to manage security incidents to minimize the blast radius
- Log management, allowing full tracking and tracing of your solutions to automatically detect and remediate any issues found
- How to accurately record and audit your infrastructure to maintain compliance with governance standards
- Data protection, covering different encryption mechanisms to ensure your data is protected at rest and in transit

Who this book is for

The AWS Certified Security – Specialty certification is recommended for those who have at least 2 years of practical AWS production deployment experience, due to the level of depth and technical ability that is expected from the candidate.

You should also have some basic knowledge of security principles and concepts and, ideally, come from a background in IT security and governance. Also, if you are responsible for maintaining and implementing AWS security across production environments and are in a position similar to the following roles, then you are ideally suited to certify in this area:

- Cloud security consultant
- Cloud security architect
- Cloud security engineers
- DevSecOps engineer
- Cloud security specialist

If you are looking to validate your knowledge of being able to architect, implement, maintain, and operate security features, techniques, and services within AWS, then this certification is the one for you!

What this book covers

`Chapter 1`, *AWS Certified Security Specialty Exam Coverage*, provides you with an understanding of the different assessment topics that will be covered throughout the exam across the five different domains, including incident response, logging and monitoring, infrastructure security, identity and access management, and data protection.

`Chapter 2`, *AWS Shared Responsibility Model*, looks at the different security models (infrastructure, container, and abstract) that define where your responsibility as a customer implementing, controlling, and managing security in AWS starts and ends, in addition to the responsibilities of AWS, which controls the security of the cloud.

`Chapter 3`, *Access Management*, outlines the core concepts of identity and access management through the use of users, groups, and roles, and the differences between them. It also dives into the different types of roles available and EC2 instance profiles, before finishing with an understanding of how to implement multi-factor authentication.

`Chapter 4`, *Working with Access Policies*, takes a deep look at the multitude of different access policies that exist across the AWS environment, and which policy type should be used in different circumstances.

You will also learn how to read JSON policies to evaluate their permissions and the steps involved to implement cross-account access.

`Chapter 5`, *Federated and Mobile Access*, provides you with a comprehensive understanding of different federated access methods, including enterprise identity and social identity federation to provide a single sign-on approach to your AWS environment. In addition, you will also be introduced to the Amazon Cognito service to understand access control through mobile applications and devices.

`Chapter 6`, *Securing EC2 Instances*, tackles the best approach to secure your instance infrastructure using a variety of techniques. These include performing vulnerability scans using Amazon Inspector, how to manage your EC2 key pairs, using AWS Systems Manager to effectively administer your fleet of EC2 instances, and also, should a security breach occur, how to isolate your EC2 instances for forensic investigation.

`Chapter 7`, *Configuring Infrastructure Security*, enables you to gain a full understanding and awareness of the range of **Virtual Private Cloud** (**VPC**) security features that AWS offers to effectively secure your VPC environments. By the end of the chapter, you will be able to confidently build a secure multi-subnet VPC using internet gateways, route tables, network access control lists, security groups, bastion hosts, NAT gateways, subnets, and virtual private gateways.

`Chapter 8`, *Implementing Application Security*, looks at how to minimize and mitigate threats against your application architecture using different AWS services to prevent them from being compromised. You will also be introduced to the configuration of securing your elastic load balancers using certificates and how to secure your APIs using AWS API Gateway.

`Chapter 9`, *DDoS Protection*, highlights how to utilize different AWS features and services to minimize threats against this very common attack to ensure that your infrastructure is not hindered or halted by the threat. You will gain an understanding of the different DDoS attack patterns and how AWS Shield can be used to provide added protection.

`Chapter 10`, *Incident Response*, explains the process and steps to manage a security incident and the best practices to help you reduce the blast radius of the attack. You will understand how to prepare for such incidents and the necessary response actions to isolate the issue using a forensic account.

`Chapter 11`, *Securing Connections to Your AWS Environment*, provides you with an understanding of the different methods of securely connecting your on-premise data centers to your AWS cloud environment using both a **Virtual Private Network** (**VPN**) and the AWS Direct Connect service.

`Chapter 12`, *Implementing Logging Mechanisms*, focuses on Amazon S3 server access logs, VPC flow logs, AWS CloudTrail logs, and the Amazon CloudWatch logging agent to enable you to track and record what is happening across your resources to allow you to monitor your environment for potential weaknesses or signs of attack indicating a security threat.

`Chapter 13`, *Auditing and Governance*, looks at the different methods and AWS services that can play key parts in helping you to maintain a level of governance and how to provide evidence during an audit. You will be introduced to AWS Artifact, the integrity controls of AWS CloudTrail, AWS Config, and how to maintain compliance with Amazon Macie.

`Chapter 14`, *Automating Security Threat Detection and Remediation*, provides you with an understanding of how to implement automation to quickly identify, record, and remediate security threats as and when they occur. It looks at Amazon CloudWatch, Amazon GuardDuty, and AWS Security Hub to help you detect and automatically resolve and block potential security incidents.

`Chapter 15`, *Discovering Security Best Practices*, covers a wide range of different methods of implementing security best practices when working with AWS in an effort to enhance your security posture. It highlights and reviews a number of common best practices that are easy to implement and could play a huge role in protecting your solutions and data.

`Chapter 16`, *Managing Key Infrastructure*, takes a deep dive look into the world of two data encryption services, the AWS **Key Management Service** (**KMS**) and CloudHSM. You will learn how to implement, manage, and secure your data through AWS encryption services and the best service to use to meet your business requirements.

`Chapter 17`, *Managing Data Security*, introduces you to a variety of different encryption features related to a range of different services covering both storage and database services, including Amazon **Elastic Block Store** (**EBS**), Amazon **Elastic File System** (**EFS**), Amazon **Simple Storage Service** (**S3**), Amazon **Relational Database Service** (**RDS**), and Amazon DynamoDB.

`Chapter 18`, *Mock Tests*, provides you with two mock exams. Each of them is 65 questions in length to review your understanding of the content covered throughout this book to help you assess your level of exam readiness.

To get the most out of this book

Throughout this book, there are a number of demonstrations that you can follow to help with your learning. As a result, I suggest you have your own AWS account created that is *not* used for any production environments. You can follow along on either a Linux-based or windows-based operating system, however, I suggest you also have the AWS CLI installed.

Software/Hardware covered in the book	**OS Requirements**
Amazon Web Services Management Console	Any device with a modern browser
AWS Command Line Interface	Linux/Windows

To create a new AWS account, please follow the guide found at: `https://aws.amazon.com/premiumsupport/knowledge-center/create-and-activate-aws-account/`.

To install the AWS CLI, please follow the guide found at: `https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-install.html`.

On completion of this book, I suggest you get as much hands-on experience with AWS as possible to use the different AWS services that are discussed to help reinforce the material from each of the chapters.

Code in Action

Code in Action videos for this book can be viewed at (`https://bit.ly/33jnvMT`).

Download the color images

We also provide a PDF file that has color images of the screenshots/diagrams used in this book. You can download it here: `http://www.packtpub.com/sites/default/files/downloads/9781789534474_ColorImages.pdf`.

Conventions used

There are a number of text conventions used throughout this book.

`CodeInText`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. Here is an example: "The `Principal` parameter is used within resource-based policies to identify the user, role, account, or federated user."

A block of code is set as follows:

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Principal": {"AWS": "arn:aws:iam::356903128354:user/Stuart"},
   "Action": "sts:AssumeRole",
   "Condition": {"Bool": {"aws:MultiFactorAuthPresent": "true"}}
 }
}
```

When we wish to draw your attention to a particular part of a code block, the relevant lines or items are set in bold:

```
[default]
exten => s,1,Dial(Zap/1|30)
exten => s,2,Voicemail(u100)
exten => s,102,Voicemail(b100)
exten => i,1,Voicemail(s0)
```

Any command-line input or output is written as follows:

```
$ mkdir css
$ cd css
```

Bold: Indicates a new term, an important word, or words that you see onscreen. For example, words in menus or dialog boxes appear in the text like this. Here is an example: "Select **Route Tables** from the menu on the left and click the blue **Create Route Table** button."

Warnings or important notes appear like this.

Tips and tricks appear like this.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, mention the book title in the subject of your message and email us at `customercare@packtpub.com`.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit `www.packtpub.com/support/errata`, selecting your book, clicking on the Errata Submission Form link, and entering the details.

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 `copyright@packt.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 `authors.packtpub.com`.

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 Packt can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about Packt, please visit `packt.com`.

1
Section 1: The Exam and Preparation

The primary objective of this section is to summarize the exam topics you will come across, along with their weighted percentages, so that you are aware of the critical points of focus.

This section comprises the following chapter:

- `Chapter 1`, *AWS Certified Security Specialty Exam Coverage*

1
AWS Certified Security Specialty Exam Coverage

The AWS Certified Security Specialty Exam has been designed to assess and validate the ability of the candidate across a number of AWS security domains to demonstrate their knowledge, awareness, understanding, and capability in securing AWS architecture, services, resources, and data.

This initial chapter will explain in detail the requirements that you need in order to pass the exam, and highlight the domains and topics that will be assessed. It is important to understand these requirements before progressing through the rest of this book to ensure that you are aware of what you will be tested on. This will allow you to determine where your strengths and weaknesses lie, thereby allowing you to spend more time on those areas.

This chapter will take you through the following topics:

- Aim of the certification
- Intended audience
- Domains accessed
- Exam details

Aim of the certification

The aim of the certification is to validate the candidate's knowledge across the following areas, as defined by AWS (source: *AWS Certified Security Specialty (SCS-C01) Exam Guide*):

- 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 the features of services used to provide a secure production environment
- Competency gained from two or more years of production deployment experience using AWS security services and features
- 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

Upon completion of this book, you will feel ready to take and sit this exam with confidence, and achieve the much sought-after AWS Certified Security – Specialty certification.

Intended audience

This exam is intended for candidates like you who are responsible for maintaining and implementing AWS security across a range of environments. Those of you in the following roles or similar would be ideally suited to attempt this certification:

- Cloud security consultant
- Cloud security architect
- Cloud security engineer
- DevSecOps engineer
- Cloud security specialist

Although these roles are typically the target audience of this certification, the certification itself is available to anyone; there are no prerequisites in terms of other certifications for taking this exam.

Domains assessed

In the exam, there are five domains that have been defined by AWS that you will be assessed against, each with a different percentage weighting level, as shown in the following table:

Domain	**Weighting level**
Incident response	12%
Logging and monitoring	20%

Infrastructure security	26%
Identity and access management	20%
Data protection	22%

Attention must be paid to each domain to ensure you feel confident and comfortable with the topics, services, and features that may crop up in your exam. Let me break down these domains further to allow you to gain a deeper understanding of exactly what is tested within each domain.

Domain 1 – Incident response

This domain tests your understanding of how best to identify, respond to, and resolve AWS incidents across a range of services, and has been broken down into the following three elements:

- **1.1: Given an AWS abuse notice, evaluate the suspected compromised instance or exposed access keys**: Here, you will be expected to know how to respond to such an incident and the steps required to remediate the issue and take the appropriate action, depending on the affected resource in question.
- **1.2: Verify that the incident response plan includes the relevant AWS services**: When an incident occurs within an AWS environment, you must be able to utilize the appropriate AWS resources to identify, isolate, and resolve the issue as quickly as possible, without affecting or hindering other AWS infrastructure and resources.
- **1.3: Evaluate the configuration of automated alerting, and execute possible remediation of security-related incidents and emerging issues**: Proactive monitoring and speed are two key elements when analyzing your infrastructure for potential issues, in addition to utilizing automated services. You must have a solid understanding of these features, and how they can assist you to spot a potential problem and help you to resolve the issue.

Being able to identity, verify, and remediate incidents as they occur within your environment allows you to effectively isolate your resources before the blast radius of the security incident travels deeper within your infrastructure.

Domain 2 – Logging and monitoring

This domain determines your ability to implement and troubleshoot solutions relating to logging, monitoring, and alerting. You will need to be able to deploy, operate, and troubleshoot solutions relating to these four components within your AWS infrastructure:

- **2.1: Design and implement security monitoring and alerting**: You must have full comprehension of the available monitoring and alerting services within AWS. In addition, you must also be aware of how these can be utilized and integrated to implement an effective solution for monitoring your infrastructure for security threats and vulnerabilities.
- **2.2: Troubleshoot security monitoring and alerting**: Implementing a monitoring and alerting system is one thing, but being able to resolve issues with the solution and design is another. You must be aware of how the architecture is coupled together and the prerequisites for specific AWS features.
- **2.3: Design and implement a logging solution**: Data held in logs generated from services and applications can provide a wealth of information to help you identify a potential security breach. Therefore, it's imperative that you have a sound awareness of how to implement a solution to capture and record log data.
- **2.4: Troubleshoot logging solutions**: Similar to 2.2, your knowledge of logging solutions has to go deeper than implementation; you have to understand the key components, concepts, and how components depend on one another to enable you to resolve any incidents.

You must understand the complexities and importance of monitoring and logging and how they can be used together as an effective security tool.

Domain 3 – Infrastructure security

The infrastructure security domain assesses your ability to architect security best practices across your AWS architecture, from an individual host, to your VPC, and then to the outer reaches of your edge infrastructure. This domain carries the highest percentage mark across your certification, so it's key that you understand all the concepts and components:

- **3.1: Design edge security on AWS**: A thorough understanding of Amazon CloudFront and its security capabilities and controls is a must, in addition to other edge services offered by AWS.

- **3.2: Design and implement a secure network infrastructure**: Here, you will be tested on your knowledge of **Virtual Private Cloud** (**VPC**) infrastructure, and how to architect an environment to meet different security needs using route tables, NACLs, bastion hosts, NAT gateways, IGWs, and security groups.
- **3.3: Troubleshoot a secure network infrastructure**: This follows on from point 3.2, which ensures that you have a deep level of security architecture, enabling you to quickly pinpoint the most likely cause of misconfiguration from a security perspective.
- **3.4: Design and implement host-based security**: This will focus on security controls that can be enabled and configured on individual hosts, such as your EC2 instances.

Implementing a VPC is one of the first elements you are likely to build within your AWS account. Understanding how to protect your VPC is key in maintaining a level of protection to the rest of your resources running within it.

Domain 4 – Identity and access management (IAM)

This domain will focus solely on everything access control-related regarding the IAM service and how to control access to your AWS resources. IAM must be understood inside out and it is essential that you have the knowledge and confidence to spot errors in IAM JSON policies:

- **4.1: Design and implement a scalable authorization and authentication system to access AWS resources**: I can't emphasize enough the importance of understanding IAM at a deep level. This point will test your knowledge of authentication and authorization mechanisms, from multi-factor authorization to implementing conditional-based IAM policies used for cross-account access.
- **4.2: Troubleshoot an authorization and authentication system to access the AWS resources domain**: Here, you will be required to demonstrate your ability to resolve complex permission-based issues with your AWS resources.

Access control is covered in detail within the exam, so you must be familiar with all things relating to access management, and specifically the IAM service. You need to be able to read access policies to determine the resulting access of that policy.

Domain 5 – Data protection

The last domain requires you to have a solid understanding and awareness of how data within AWS can be protected through an encryption mechanism, both at rest and in transit. You will be assessed on services relating to encryption, specifically the **Key Management Service** (**KMS**):

- **5.1: Design and implement key management and use**: This point requires you to demonstrate your knowledge when it comes to encryption using KMS. You must be aware of when, how, and why this service is used, and which services can benefit from the features it offers.
- **5.2: Troubleshoot key management**: Data encryption keys are a powerful tool to help protect your data, but you must understand how you can configure the permissions surrounding these keys and what to look for when troubleshooting issues relating to data encryption and customer master keys.
- **5.3: Design and implement a data encryption solution for data at rest and data in transit**: Here, you will be assessed on your understanding of encryption as a whole. You must demonstrate that you have the knowledge to encrypt data in any state using the correct configuration, depending on a set of requirements.

It is of no surprise that the security specialty will assess your understanding of encryption, which will be centered around two key services, AWS **Key Management Service** (**KMS**) and AWS CloudHSM. The KMS service integrates with many different AWS services to offer a level of encryption, so make sure that you are familiar with all the components of KMS.

Exam details

Much like all other AWS certifications, the format consists of multiple choice questions. You will have 170 minutes to answer 65 questions, which is just over 2.5 minutes per question. You should have plenty of time, provided you have studied well and are confident in the domain areas I just discussed.

Some questions can be scenario-based and do take a little longer to process and answer, but don't panic; focus on what's being asked and eliminate the obviously wrong answers. It is likely there are two that you can rule out. Take your time and re-read the question before deciding on your final answer.

The passing score for this certification is 750 out of 1000 (75%). The exam itself is USD 300 and it must be taken at an AWS authorized testing center, which can all be booked online through the AWS website, at: `https://aws.amazon.com/certification/`.

Summary

In this chapter, I primarily focused on the different domains that you will be assessed against when taking your exam. I wanted to provide a deeper understanding of what each of the domain points might assess you against in order to allow you to understand where your strengths and weaknesses might lie. As you progress through the chapters, you will gain an understanding sufficient to cover all elements that have been discussed within this chapter to ensure that you are prepared for your certification.

In the next chapter, we begin by looking at the foundation of security on AWS, the AWS shared responsibility model, and how an understanding of this plays an important part in understanding AWS security as a whole.

Questions

As we conclude, here is a list of questions for you to test your knowledge regarding this chapter's material. You will find the answers in the *Assessments* section of the *Appendix*:

1. True or false: You need to complete a few other certifications as a prerequisite for the AWS Certified Security – Specialty certification.
2. How many domains have been defined by AWS that you will be assessed against in the exam?
3. The AWS Certified Security – Specialty certification consists of how many questions? (choose any one)
    - 55 questions
    - 60 questions
    - 65 questions
    - 75 questions

Further reading

For more information on this certification, please visit the AWS site, where you can download the exam guide and sample questions, at: `https://aws.amazon.com/certification/certified-security-specialty/`.