Third Edition

AWS Certified Solutions Architect

STUDY GUIDE

ASSOCIATE (SAA-C02) 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

BEN PIPER
DAVID CLINTON

SYBEX
A Wiley Brand

AWS
Certified Solutions Architect Study Guide
Associate (SAA-C02) Exam
Third Edition

Ben Piper
David Clinton

SYBEX®
A Wiley Brand

Copyright © 2021 by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-71308-1
ISBN: 978-1-119-71309-8 (ebk.)
ISBN: 978-1-119-71310-4 (ebk.)

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 646-8600. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at www.wiley.com/go/permissions.

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: 2020947039

TRADEMARKS: Wiley, the Wiley logo, and the Sybex logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. AWS is a registered trademark of Amazon Technologies, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Acknowledgments

We would like to thank the following people who helped us create *AWS Certified Solutions Architect Study Guide: Associate SAA-C02 Exam, Third Edition*.

First, a special thanks to our friends at Wiley. Kenyon Brown, senior acquisitions editor, got the ball rolling on this project and pushed to get this book published quickly. His experience and guidance throughout the project was critical. Stephanie Barton, project editor, helped push this book forward by keeping us accountable to our deadlines. Her edits made many of the technical parts of this book more readable.

Todd Montgomery reviewed the chapters and questions for technical accuracy. Not only did his comments and suggestions make this book more accurate, he also provided additional ideas for the chapter review questions to make them more challenging and relevant to the exam.

Lastly, the authors would like to thank each other!

About the Authors

Ben Piper is a networking and cloud consultant who has authored multiple books, including the *AWS Certified Cloud Practitioner Study Guide: Foundational CLF-C01 Exam* (Sybex, 2019) and *Learn Cisco Network Administration in a Month of Lunches* (Manning, 2017). You can contact Ben by visiting his website: `benpiper.com`.

David Clinton is a Linux server admin and AWS solutions architect who has worked with IT infrastructure in both academic and enterprise environments. He has authored books—including (with Ben Piper) the *AWS Certified Cloud Practitioner Study Guide: Foundational CLF-C01 Exam* (Sybex, 2019) and *Linux in Action* (Manning Publications, 2018)—and created more than two dozen video courses teaching Amazon Web Services and Linux administration, server virtualization, and IT security for Pluralsight.

In a "previous life," David spent 20 years as a high school teacher. He currently lives in Toronto, Canada, with his wife and family and can be reached through his website: `bootstrap-it.com`.

Contents at a Glance

Introduction		*xxi*
Assessment Test		*xxvii*
Part I	**The Core AWS Services**	**1**
Chapter 1	Introduction to Cloud Computing and AWS	3
Chapter 2	Amazon Elastic Compute Cloud and Amazon Elastic Block Store	21
Chapter 3	AWS Storage	59
Chapter 4	Amazon Virtual Private Cloud	83
Chapter 5	Database Services	133
Chapter 6	Authentication and Authorization—AWS Identity and Access Management	165
Chapter 7	CloudTrail, CloudWatch, and AWS Config	183
Chapter 8	The Domain Name System and Network Routing: Amazon Route 53 and Amazon CloudFront	211
Chapter 9	Simple Queue Service and Kinesis	233
Part II	**The Well-Architected Framework**	**245**
Chapter 10	The Reliability Pillar	247
Chapter 11	The Performance Efficiency Pillar	273
Chapter 12	The Security Pillar	301
Chapter 13	The Cost Optimization Pillar	335
Chapter 14	The Operational Excellence Pillar	353
Appendix	Answers to Review Questions	385
Index		*415*

Contents

Introduction *xxi*

Assessment Test *xxvii*

Part I The Core AWS Services 1

Chapter 1 Introduction to Cloud Computing and AWS 3

Cloud Computing and Virtualization 4
- Cloud Computing Architecture 4
- Cloud Computing Optimization 5

The AWS Cloud 6
AWS Platform Architecture 10
AWS Reliability and Compliance 12
- The AWS Shared Responsibility Model 12
- The AWS Service Level Agreement 13

Working with AWS 13
- The AWS CLI 14
- AWS SDKs 14
- Technical Support and Online Resources 14
- Support Plans 14
- Other Support Resources 15

Summary 15
Exam Essentials 16
Review Questions 17

Chapter 2 Amazon Elastic Compute Cloud and Amazon Elastic Block Store 21

Introduction 22
EC2 Instances 22
- Provisioning Your Instance 23
- Configuring Instance Behavior 28
- Placement Groups 28
- Instance Pricing 29
- Instance Lifecycle 30
- Resource Tags 30
- Service Limits 31

EC2 Storage Volumes 32
- Elastic Block Store Volumes 32
- Instance Store Volumes 34

Accessing Your EC2 Instance 35

Securing Your EC2 Instance 36
Security Groups 36
IAM Roles 37
NAT Devices 37
Key Pairs 38
EC2 Auto Scaling 38
Launch Configurations 39
Launch Templates 39
Auto Scaling Groups 40
Auto Scaling Options 42
AWS Systems Manager 46
Actions 47
Insights 49
AWS CLI Example 51
Summary 52
Exam Essentials 53
Review Questions 54

Chapter 3 AWS Storage 59

Introduction 60
S3 Service Architecture 61
Prefixes and Delimiters 61
Working with Large Objects 61
Encryption 62
Logging 63
S3 Durability and Availability 64
Durability 64
Availability 65
Eventually Consistent Data 65
S3 Object Lifecycle 66
Versioning 66
Lifecycle Management 66
Accessing S3 Objects 67
Access Control 67
Presigned URLs 69
Static Website Hosting 69
Amazon S3 Glacier 71
Storage Pricing 72
Other Storage-Related Services 73
Amazon Elastic File System 73
Amazon FSx 73
AWS Storage Gateway 73
AWS Snowball 74
AWS DataSync 74
AWS CLI Example 75

Summary 76
Exam Essentials 77
Review Questions 78

Chapter 4 Amazon Virtual Private Cloud 83

Introduction 84
VPC CIDR Blocks 84
Secondary CIDR Blocks 85
IPv6 CIDR Blocks 85
Subnets 87
Subnet CIDR Blocks 87
Availability Zones 88
IPv6 CIDR Blocks 91
Elastic Network Interfaces 91
Primary and Secondary Private IP Addresses 91
Attaching Elastic Network Interfaces 91
Enhanced Networking 93
Internet Gateways 93
Route Tables 94
Routes 94
The Default Route 95
Security Groups 98
Inbound Rules 98
Outbound Rules 99
Sources and Destinations 99
Stateful Firewall 99
Default Security Group 100
Network Access Control Lists 101
Inbound Rules 102
Outbound Rules 105
Using Network Access Control Lists and Security Groups Together 106
Public IP Addresses 106
Elastic IP Addresses 107
AWS Global Accelerator 109
Network Address Translation 109
Network Address Translation Devices 110
Configuring Route Tables to Use NAT Devices 112
NAT Gateway 113
NAT Instance 113
VPC Peering 114
Hybrid Cloud Networking 115
Virtual Private Networks 115
AWS Transit Gateway 115
AWS Direct Connect 123

High-Performance Computing 125
Elastic Fabric Adapter 125
AWS ParallelCluster 126
Summary 126
Exam Essentials 127
Review Questions 129

Chapter 5 Database Services 133

Introduction 134
Relational Databases 134
Columns and Attributes 135
Using Multiple Tables 135
Structured Query Language 137
Online Transaction Processing vs. Online Analytic Processing 137
Amazon Relational Database Service 138
Database Engines 138
Licensing Considerations 139
Database Option Groups 140
Database Instance Classes 140
Storage 141
Read Replicas 145
High Availability (Multi-AZ) 146
Single-Master 147
Multi-Master 147
Backup and Recovery 148
Automated Snapshots 148
Maintenance Items 149
Amazon Redshift 149
Compute Nodes 149
Data Distribution Styles 150
Redshift Spectrum 150
AWS Database Migration Service 150
Nonrelational (NoSQL) Databases 151
Storing Data 151
Querying Data 152
Types of Nonrelational Databases 152
DynamoDB 153
Partition and Hash Keys 153
Attributes and Items 154
Throughput Capacity 155
Reading Data 157
Global Tables 158
Backups 158
Summary 158

Exam Essentials 159
Review Questions 161

Chapter 6 Authentication and Authorization—AWS Identity and Access Management 165

Introduction 166
IAM Identities 166
IAM Policies 167
User and Root Accounts 168
Access Keys 170
Groups 172
Roles 173
Authentication Tools 173
Amazon Cognito 174
AWS Managed Microsoft AD 174
AWS Single Sign-On 174
AWS Key Management Service 175
AWS Secrets Manager 175
AWS CloudHSM 175
AWS CLI Example 176
Summary 177
Exam Essentials 177
Review Questions 179

Chapter 7 CloudTrail, CloudWatch, and AWS Config 183

Introduction 184
CloudTrail 185
Management Events 185
Data Events 186
Event History 186
Trails 186
Log File Integrity Validation 189
CloudWatch 189
CloudWatch Metrics 190
Graphing Metrics 192
Metric Math 194
CloudWatch Logs 195
CloudWatch Alarms 198
Amazon EventBridge 201
AWS Config 202
The Configuration Recorder 203
Configuration Items 203
Configuration History 203
Configuration Snapshots 203
Monitoring Changes 204

Summary 206
Exam Essentials 206
Review Questions 207

Chapter 8 The Domain Name System and Network Routing: Amazon Route 53 and Amazon CloudFront 211

Introduction 212
The Domain Name System 212
Namespaces 212
Name Servers 213
Domains and Domain Names 213
Domain Registration 214
Domain Layers 214
Fully Qualified Domain Names 214
Zones and Zone Files 215
Record Types 215
Alias Records 216
Amazon Route 53 216
Domain Registration 217
DNS Management 217
Availability Monitoring 219
Routing Policies 220
Traffic Flow 222
Route 53 Resolver 223
Amazon CloudFront 223
AWS CLI Example 225
Summary 226
Exam Essentials 226
Review Questions 228

Chapter 9 Simple Queue Service and Kinesis 233

Introduction 234
Simple Queue Service 234
Queues 234
Queue Types 235
Polling 236
Dead-Letter Queues 237
Kinesis 237
Kinesis Video Streams 237
Kinesis Data Streams 238
Kinesis Data Firehose 239
Kinesis Data Firehose vs. Kinesis Data Streams 239
Summary 240
Exam Essentials 240
Review Questions 241

Part II The Well-Architected Framework 245

Chapter 10 The Reliability Pillar 247

Introduction 248
Calculating Availability 248
Availability Differences in Traditional vs. Cloud-Native Applications 249
Know Your Limits 252
Increasing Availability 252
EC2 Auto Scaling 253
Launch Configurations 253
Launch Templates 254
Auto Scaling Groups 255
Auto Scaling Options 256
Data Backup and Recovery 261
S3 261
Elastic File System 261
Elastic Block Storage 261
Database Resiliency 262
Creating a Resilient Network 263
VPC Design Considerations 263
External Connectivity 263
Designing for Availability 264
Designing for 99 Percent Availability 264
Designing for 99.9 Percent Availability 265
Designing for 99.99 Percent Availability 266
Summary 267
Exam Essentials 268
Review Questions 269

Chapter 11 The Performance Efficiency Pillar 273

Introduction 274
Optimizing Performance for the Core AWS Services 274
Compute 275
Storage 279
Database 282
Network Optimization and Load Balancing 284
Infrastructure Automation 286
CloudFormation 286
Third-Party Automation Solutions 288
Reviewing and Optimizing Infrastructure Configurations 289
Load Testing 289
Visualization 290

Optimizing Data Operations 291
Caching 291
Partitioning/Sharding 293
Compression 294
Summary 294
Exam Essentials 295
Review Questions 297

Chapter 12 The Security Pillar 301

Introduction 302
Identity and Access Management 302
Protecting AWS Credentials 303
Fine-Grained Authorization 303
Permissions Boundaries 305
Roles 306
Enforcing Service-Level Protection 313
Detective Controls 313
CloudTrail 313
CloudWatch Logs 314
Searching Logs with Athena 315
Auditing Resource Configurations with AWS Config 317
Amazon GuardDuty 318
Amazon Inspector 321
Amazon Detective 322
Security Hub 323
Protecting Network Boundaries 323
Network Access Control Lists and Security Groups 323
AWS Web Application Firewall 323
AWS Shield 324
Data Encryption 324
Data at Rest 325
Data in Transit 326
Macie 327
Summary 327
Exam Essentials 328
Review Questions 329

Chapter 13 The Cost Optimization Pillar 335

Introduction 336
Planning, Tracking, and Controlling Costs 336
AWS Budgets 337
Monitoring Tools 338
AWS Organizations 339

AWS Trusted Advisor 340
Online Calculator Tools 340
Cost-Optimizing Compute 342
Maximizing Server Density 343
EC2 Reserved Instances 343
EC2 Spot Instances 344
Auto Scaling 347
Elastic Block Store Lifecycle Manager 347
Summary 347
Exam Essentials 348
Review Questions 349

Chapter 14 The Operational Excellence Pillar 353

Introduction 354
CloudFormation 354
Creating Stacks 355
Deleting Stacks 356
Using Multiple Stacks 356
Stack Updates 359
Preventing Updates to Specific Resources 360
Overriding Stack Policies 361
CodeCommit 361
Creating a Repository 362
Repository Security 362
Interacting with a Repository Using Git 363
CodeDeploy 365
The CodeDeploy Agent 366
Deployments 366
Deployment Groups 366
Deployment Types 366
Deployment Configurations 367
Lifecycle Events 368
The Application Specification File 369
Triggers and Alarms 370
Rollbacks 370
CodePipeline 371
Continuous Integration 371
Continuous Delivery 371
Creating the Pipeline 372
Artifacts 373
AWS Systems Manager 374
Actions 374
Insights 377

AWS Landing Zone 378
Summary 379
Exam Essentials 379
Review Questions 381

Appendix Answers to Review Questions 385

Chapter 1: Introduction to Cloud Computing and AWS 386
Chapter 2: Amazon Elastic Compute Cloud and Amazon Elastic Block Store 387
Chapter 3: AWS Storage 389
Chapter 4: Amazon Virtual Private Cloud 391
Chapter 5: Database Services 393
Chapter 6: Authentication and Authorization—AWS Identity and Access Management 395
Chapter 7: CloudTrail, CloudWatch, and AWS Config 397
Chapter 8: The Domain Name System and Network Routing: Amazon Route 53 and Amazon CloudFront 399
Chapter 9: Simple Queue Service and Kinesis 401
Chapter 10: The Reliability Pillar 403
Chapter 11: The Performance Efficiency Pillar 405
Chapter 12: The Security Pillar 407
Chapter 13: The Cost Optimization Pillar 409
Chapter 14: The Operational Excellence Pillar 411

Index *415*

Table of Exercises

Exercise 1.1 Use the AWS CLI 16

Exercise 2.1 Launch an EC2 Linux Instance and Log in Using SSH 27

Exercise 2.2 Assess the Free Capacity of a Running Instance and Change Its Instance Type 27

Exercise 2.3 Assess Which Pricing Model Will Best Meet the Needs of a Deployment 30

Exercise 2.4 Create and Launch an AMI Based on an Existing Instance Storage Volume 34

Exercise 2.5 Create a Launch Template 40

Exercise 2.6 Install the AWS CLI and Use It to Launch an EC2 Instance 51

Exercise 2.7 Clean Up Unused EC2 Resources 52

Exercise 3.1 Create a New S3 Bucket and Upload a File 62

Exercise 3.2 Enable Versioning and Lifecycle Management for an S3 Bucket 67

Exercise 3.3 Generate and Use a Presigned URL 69

Exercise 3.4 Enable Static Website Hosting for an S3 Bucket 70

Exercise 3.5 Calculate the Total Lifecycle Costs for Your Data 73

Exercise 4.1 Create a New VPC 85

Exercise 4.2 Create a New Subnet 89

Exercise 4.3 Create and Attach a Primary ENI 92

Exercise 4.4 Create an Internet Gateway and Default Route 96

Exercise 4.5 Create a Custom Security Group 100

Exercise 4.6 Create an Inbound Rule to Allow Remote Access from Any IP Address 103

Exercise 4.7 Allocate and Use an Elastic IP Address 107

Exercise 4.8 Create a Transit Gateway 117

Exercise 4.9 Create a Blackhole Route 122

Exercise 5.1 Create an RDS Database Instance 143

Exercise 5.2 Create a Read Replica 145

Exercise 5.3 Promote the Read Replica to a Master 146

Exercise 5.4 Create a Table in DynamoDB Using Provisioned Mode 156

Exercise 6.1 Lock Down the Root User 169

Exercise 6.2 Assign and Implement an IAM Policy 169

Exercise 6.3 Create, Use, and Delete an AWS Access Key 171

Exercise 6.4 Create and Configure an IAM Group 172

Exercise 7.1 Create a Trail 187
Exercise 7.2 Create a Graph Using Metric Math 194
Exercise 7.3 Deliver CloudTrail Logs to CloudWatch Logs 197
Exercise 8.1 Create a Hosted Zone on Route 53 for an EC2 Web Server 218
Exercise 8.2 Set Up a Health Check 219
Exercise 8.3 Configure a Route 53 Routing Policy 221
Exercise 8.4 Create a CloudFront Distribution for Your S3-Based Static Website . . . 224
Exercise 10.1 Create a Launch Template 254
Exercise 11.1 Configure and Launch an Application Using Auto Scaling 277
Exercise 11.2 Sync Two S3 Buckets as Cross-Region Replicas. 281
Exercise 11.3 Upload to an S3 Bucket Using Transfer Acceleration. 282
Exercise 11.4 Create and Deploy an EC2 Load Balancer 285
Exercise 11.5 Launch a Simple CloudFormation Template 287
Exercise 11.6 Create a CloudWatch Dashboard 290
Exercise 12.1 Create a Limited Administrative User 305
Exercise 12.2 Create and Assume a Role as an IAM User 311
Exercise 12.3 Configure VPC Flow Logging. 315
Exercise 12.4 Encrypt an EBS Volume 325
Exercise 13.1 Create an AWS Budget to Send an Alert 338
Exercise 13.2 Build Your Own Stack in Simple Monthly Calculator 341
Exercise 13.3 Request a Spot Fleet Using the AWS CLI. 345
Exercise 14.1 Create a Nested Stack 357
Exercise 14.2 Create and Interact with a CodeCommit Repository 363

Introduction

Studying for any certification always involves deciding how much of your studying should be practical hands-on experience and how much should be simply memorizing facts and figures. Between the two of us, we've taken dozens of IT certification exams, so we know how important it is to use your study time wisely. We've designed this book to help you discover your strengths and weaknesses on the AWS platform so that you can focus your efforts properly. Whether you've been working with AWS for a long time or whether you're relatively new to it, we encourage you to carefully read this book from cover to cover.

Passing the AWS Certified Solutions Architect – Associate exam requires understanding the components and operation of the core AWS services as well as how those services interact with each other. Read through the official documentation for the various AWS services. Amazon offers HTML, PDF, and Kindle documentation for many of them. Use this book as a guide to help you identify your strengths and weaknesses so that you can focus your study efforts properly.

You should have at least six months of hands-on experience with AWS before taking the AWS Certified Solutions Architect – Associate exam. If you're relatively new to AWS, we strongly recommend our own *AWS Certified Cloud Practitioner Study Guide: CLF-C01 Exam* (Sybex, 2019) as a primer.

Even though this book is designed specifically for the AWS Certified Solutions Architect – Associate exam, some of your fellow readers have found it useful for preparing for the SysOps Administrator and DevOps Engineer exams.

Hands-on experience is crucial for exam success. Each chapter in this *AWS Certified Solutions Architect Study Guide: Associate SAA-C02 Exam, Third Edition* contains hands-on exercises that you should strive to complete during or immediately after you read the chapter. It's vital to understand that the exercises don't cover every possible scenario for every AWS service. In fact, it's quite the opposite. The exercises provide you with a foundation to build on. Use them as your starting point, but don't be afraid to venture out on your own. Feel free to modify them to match the variables and scenarios you might encounter in your own organization. Keep in mind that some of the exercises and figures use the AWS web console, which is in constant flux. As such, screenshots and step-by-step details of exercises may change. Use these eventualities as excuses to dig into the AWS online documentation and browse around the web console on your own. Also remember that although you can complete many of the exercises within the bounds of the AWS Free Tier, getting enough practice to pass the exam will likely require you to spend some money. But it's money well spent, as getting certified is an investment in your career and your future.

Each chapter contains review questions to thoroughly test your understanding of the services and concepts covered in that chapter. They also test your ability to integrate the concepts with information from preceding chapters. Although the difficulty of the questions varies, rest assured that they are not "fluff." We've designed the questions to help you realistically gauge your understanding and readiness for the exam. Avoid the temptation to rush through the questions to just get to the answers. Once you complete the assessment in

each chapter, referring to the answer key will give you not only the correct answers but a detailed explanation as to why they're correct. It will also explain why the other answers are incorrect.

The book also contains a self-assessment exam with 39 questions, two practice exams with 50 questions each to help you gauge your readiness to take the exam, and flashcards to help you learn and retain key facts needed to prepare for the exam.

This *AWS Certified Solutions Architect Study Guide: Associate SAA-C02 Exam, Third Edition* is divided into two parts: "The Core AWS Services" and "The Well-Architected Framework."

Part I, "The Core AWS Services"

The first part of the book dives deep into each of the core AWS services. These services include ones you probably already have at least a passing familiarity with: Elastic Compute Cloud (EC2), Virtual Private Cloud (VPC), Identity and Access Management (IAM), Route 53, and Simple Storage Service (S3), to name just a few.

Some AWS services seem to serve similar or even nearly identical purposes. You'll learn about the subtle but important differences between seemingly similar services and, most importantly, when to use each.

Part II, "The Well-Architected Framework"

The second part of the book is a set of best practices and principles aimed at helping you design, implement, and operate systems in the cloud. Part II focuses on the following five pillars of good design:

- Reliability
- Performance efficiency
- Security
- Cost optimization
- Operational excellence

Each chapter of Part II revisits the core AWS services in light of a different pillar. Also, because not every AWS service is large enough to warrant its own chapter, Part II simultaneously introduces other services that, although less well known, may still show up on the exam.

Achieving the right balance among these pillars is a key skill you need to develop as a solutions architect. Prior to beginning Part II, we encourage you to peruse the Well-Architected Framework white paper, which is available for download at `d0.awsstatic.com/whitepapers/architecture/AWS_Well-Architected_Framework.pdf`.

What Does This Book Cover?

This book covers topics you need to know to prepare for the Amazon Web Services (AWS) Certified Solutions Architect – Associate exam:

Chapter 1: Introduction to Cloud Computing and AWS This chapter provides an overview of the AWS Cloud computing platform and its core services and concepts.

Chapter 2: Amazon Elastic Compute Cloud and Amazon Elastic Block Store This chapter covers EC2 instances—the virtual machines that you can use to run Linux and Windows workloads on AWS. It also covers the Elastic Block Store service that EC2 instances depend on for persistent data storage.

Chapter 3: AWS Storage In this chapter, you'll learn about Simple Storage Service (S3) and Glacier, which provide unlimited data storage and retrieval for AWS services, your applications, and the Internet.

Chapter 4: Amazon Virtual Private Cloud This chapter explains Amazon Virtual Private Cloud (Amazon VPC), a virtual network that contains network resources for AWS services.

Chapter 5: Database Services In this chapter, you will learn about some different managed database services offered by AWS, including Relational Database Service (RDS), DynamoDB, and Redshift.

Chapter 6: Authentication and Authorization—AWS Identity and Access Management This chapter covers AWS Identity and Access Management (IAM), which provides the primary means for protecting the AWS resources in your account.

Chapter 7: CloudTrail, CloudWatch, and AWS Config In this chapter, you'll learn how to log, monitor, and audit your AWS resources.

Chapter 8: The Domain Name System and Network Routing: Amazon Route 53 and Amazon CloudFront This chapter focuses on the Domain Name System (DNS) and Route 53, the service that provides public and private DNS hosting for both internal AWS resources and the Internet. It also covers CloudFront, Amazon's global content delivery network.

Chapter 9: Simple Queue Service and Kinesis This chapter explains how to use the principle of loose coupling to create scalable and highly available applications. You'll learn how Simple Queue Service (SQS) and Kinesis fit into the picture.

Chapter 10: The Reliability Pillar This chapter will show you how to architect and integrate AWS services to achieve a high level of reliability for your applications. You'll learn how to plan around and recover from inevitable outages to keep your systems up and running.

Chapter 11: The Performance Efficiency Pillar This chapter covers how to build highly performing systems and use the AWS elastic infrastructure to rapidly scale up and out to meet peak demand.

Chapter 12: The Security Pillar In this chapter, you'll learn how to use encryption and security controls to protect the confidentiality, integrity, and availability of your data and systems on AWS. You'll also learn about the various security services such as GuardDuty, Inspector, Shield, and Web Application Firewall.

Chapter 13: The Cost Optimization Pillar This chapter will show you how to estimate and control your costs in the cloud.

Chapter 14: The Operational Excellence Pillar In this chapter, you'll learn how to keep your systems running smoothly on AWS. You'll learn how to implement a DevOps mind-set using CloudFormation, Systems Manager, and the AWS Developer Tools.

Interactive Online Learning Environment and Test Bank

The authors have worked hard to provide some really great tools to help you with your certification process. The interactive online learning environment that accompanies the *AWS Certified Solutions Architect Study Guide: Associate SAA-C02 Exam, Third Edition* provides a test bank with study tools to help you prepare for the certification exam—and increase your chances of passing it the first time! The test bank includes the following:

Sample Tests All the questions in this book are provided, including the assessment test at the end of this Introduction and the chapter tests that include the review questions at the end of each chapter. In addition, there are two practice exams with 50 questions each. Use these questions to test your knowledge of the study guide material. The online test bank runs on multiple devices.

Flashcards The online text banks include 100 flashcards specifically written to hit you hard, so don't get discouraged if you don't ace your way through them at first. They're there to ensure that you're really ready for the exam. And no worries—armed with the review questions, practice exams, and flashcards, you'll be more than prepared when exam day comes. Questions are provided in digital flashcard format (a question followed by a single correct answer). You can use the flashcards to reinforce your learning and provide last-minute test prep before the exam.

Resources You'll find some AWS CLI and other code examples from the book for you to cut and paste for use in your own environment. A glossary of key terms from this book is also available as a fully searchable PDF.

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

Exam Objectives

The AWS Certified Solutions Architect – Associate exam is intended for people who have experience in designing distributed applications and systems on the AWS platform. In general, you should have the following before taking the exam:

- A minimum of one year of hands-on experience designing systems on AWS
- Hands-on experience using the AWS services that provide compute, networking, storage, and databases
- Ability to define a solution using architectural design principles based on customer requirements
- Ability to provide implementation guidance
- Ability to identify which AWS services meet a given technical requirement
- An understanding of the five pillars of the Well-Architected Framework
- An understanding of the AWS global infrastructure, including the network technologies used to connect them
- An understanding of AWS security services and how they integrate with traditional on-premises security infrastructure

The exam covers five different domains, with each domain broken down into objectives.

Objective Map

The following table lists each domain and its weighting in the exam, along with the chapters in the book where that domain's objectives are covered.

Domain	Percentage of Exam	Chapters
Domain 1: Design Resilient Architectures	30%	
1.1 Design a multi-tier architecture solution		2, 3, 5, 8, 9, 10, 11
1.2 Design highly available and/or fault-tolerant architectures		2, 3, 5, 7, 8, 9, 10, 11, 14

Domain	Percentage of Exam	Chapters
1.3 Design decoupling mechanisms using AWS services		4, 5, 9, 10, 11, 14
1.4 Choose appropriate resilient storage		2, 3, 5, 9, 10, 11
Domain 2: Design High-Performing Architectures	28%	
2.1 Identify elastic and scalable compute solutions for a workload		2, 3, 5, 7, 8, 9, 11
2.2 Select high-performing and scalable storage solutions for a workload		2, 3, 9, 11
2.3 Select high-performing networking solutions for a workload		5, 8, 9, 11
2.4 Choose high-performing database solutions for a workload		5, 11
Domain 3: Design Secure Applications and Architectures	24%	
3.1 Design secure access to AWS resources		2, 3, 4, 6, 7, 12
3.2 Design secure application tiers		3, 6, 12
3.3 Select appropriate data security options		3, 4, 6, 7, 12
Domain 4: Design Cost-Optimized Architectures	18%	
4.1 Identify cost-effective storage solutions		2, 3, 13
4.2 Identify cost-effective compute and database services		2, 13
4.3 Design cost-optimized network architectures		8, 13

Assessment Test

1. True/false: The Developer Support plan provides access to a support application programming interface (API).
   - **A.** True
   - **B.** False
2. True/false: AWS is responsible for managing the network configuration of your EC2 instances.
   - **A.** True
   - **B.** False
3. Which of the following services is most useful for decoupling the components of a monolithic application?
   - **A.** SNS
   - **B.** KMS
   - **C.** SQS
   - **D.** Glacier
4. An application you want to run on EC2 requires you to license it based on the number of physical CPU sockets and cores on the hardware you plan to run the application on. Which of the following tenancy models should you specify?
   - **A.** Dedicated host
   - **B.** Dedicated instance
   - **C.** Shared tenancy
   - **D.** Bring your own license
5. True/false: Changing the instance type of an EC2 instance will change its elastic IP address.
   - **A.** True
   - **B.** False
6. True/false: You can use a Quick Start Amazon Machine Image (AMI) to create any instance type.
   - **A.** True
   - **B.** False
7. Which S3 encryption option does *not* require AWS persistently storing the encryption keys it uses to decrypt data?
   - **A.** Client-side encryption
   - **B.** SSE-KMS
   - **C.** SSE-S3
   - **D.** SSE-C

8. True/false: Durability measures the percentage of likelihood that a given object will not be inadvertently lost by AWS over the course of a year.
   A. True
   B. False

9. True/false: After uploading a new object to S3, there will be a slight delay (one to two seconds) before the object is available.
   A. True
   B. False

10. You created a Virtual Private Cloud (VPC) using the Classless Inter-Domain Routing (CIDR) block 10.0.0.0/24. You need to connect to this VPC from your internal network, but the IP addresses in use on your internal network overlap with the CIDR. Which of the following is a valid way to address this problem?
    A. Remove the CIDR and use IPv6 instead.
    B. Change the VPC's CIDR.
    C. Create a new VPC with a different CIDR.
    D. Create a secondary CIDR for the VPC.

11. True/false: An EC2 instance must be in a public subnet to access the Internet.
    A. True
    B. False

12. True/false: The route table for a public subnet must have a default route pointing to an Internet gateway as a target.
    A. True
    B. False

13. Which of the following use cases is well suited for DynamoDB?
    A. Running a MongoDB database on AWS
    B. Storing large binary files exceeding 1 GB in size
    C. Storing JSON documents that have a consistent structure
    D. Storing image assets for a website

14. True/false: You can create a DynamoDB global secondary index for an existing table at any time.
    A. True
    B. False

15. True/false: Enabling point-in-time RDS snapshots is sufficient to give you a recovery point objective (RPO) of less than 10 minutes.
    A. True
    B. False