

Sidhartha Chauhan, James Devine,  
Alan Halachmi, Matt Lehwess,  
Nick Matthews, Steve Morad,  
Steve Seymour

# AWS® Certified Advanced Networking OFFICIAL STUDY GUIDE

**SPECIALTY EXAM**

Covers exam objectives, including designing, developing, and deploying cloud-based solutions; implementing core services following architectural best practices; designing and maintaining network architecture for all services; leveraging tools to automate network configuration; and much more...

Includes interactive online learning environment and study tools with:

- + 2 custom practice exams
- + 100 electronic flashcards
- + Searchable key term glossary



# **AWS<sup>®</sup>**

# **Certified Advanced Networking**

## **Official Study Guide**





# **AWS<sup>®</sup>**

## **Certified Advanced Networking**

### **Official Study Guide Specialty Exam**



Sidhartha Chauhan, James Devine,  
Alan Halachmi, Matt Lehwess, Nick Matthews,  
Steve Morad, Steve Seymour



Senior Acquisitions Editor: Kenyon Brown  
Project Editor: Gary Schwartz  
Copy Editor: Kezia Endsley  
Editorial Manager: Pete Gaughan and Mary Beth Wakefield  
Production Manager: Kathleen Wisor  
Executive Editor: Jim Minatel  
Book Designers: Judy Fung and Bill Gibson  
Proofreader: Nancy Carrasco  
Indexer: Johnna VanHoose Dinse  
Project Coordinator, Cover: Brent Savage  
Cover Designer: Wiley  
Cover Image: ©Jeremy Woodhouse/Getty Images, Inc.

Copyright © 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.  
Published by John Wiley & Sons, Inc., Indianapolis, Indiana

Published simultaneously in Canada

ISBN: 978-1-119-43983-7

ISBN: 978-1-119-43988-2 (ebk.)

ISBN: 978-1-119-43990-5 (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 <http://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 <http://booksupport.wiley.com>. For more information about Wiley products, visit [www.wiley.com](http://www.wiley.com).

**Library of Congress Control Number:** 2017962409

**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.

10 9 8 7 6 5 4 3 2 1

*To those who designed and built what we explain herein.*





# Acknowledgments

The authors would like to thank a few people who helped us develop and write this AWS Certified Advanced Networking – Specialty Official Study Guide.

First, thanks to all of our families for supporting us in our seemingly endless efforts to produce this book. We know the hours away from home were only possible because of you. The readers of this book owe you a debt of gratitude, as well.

A huge thanks to our colleagues, Dave Cuthbert and Dave Walker, who guest authored the chapters on automation and risk and compliance, respectively. Many thanks to James Hamilton for the Foreword and to Mark Ryland and Camil Samaha for their cover-to-cover contributions.

When we wrote this book, many of the features and services described were only on the drawing board. Thanks to the product and engineering teams for taking the time to provide us with insight into new and exciting capabilities. Our readers thank you, too!

Of course, we must thank all of the supporting team members who helped shepherd us to the finish line: Nathan Bower and Victoria Steidel, our thoughtful technical editors, who reviewed and edited all of the content; Mary Kay Sondecker, who answered our call for project help; and Sharon Saturnus, our project manager, who had the task of herding cats – the authors.



# About the Authors



**Sidhartha Chauhan**, Solutions Architect, Amazon Web Services

Sid works with enterprise customers to design highly-scalable cloud architectures. He has a special inclination toward computer networking technologies and holds a master's degree in computer networking from North Carolina State University, along with various leading industry certifications. Before joining Amazon, Sid worked with a large telecommunications organization designing large-scale Local Area Network (LAN)/Wide Area Network (WAN) networks. In his free time, Sid plays

guitar for an award-winning New York City-based Indian band called “Rhythm Tolee.” He also enjoys photography and fitness.



**James Devine**, Solutions Architect, Amazon Web Services

Using AWS to help design solutions for nonprofit customers who are making a difference in the world is what keeps James motivated. He holds a bachelor's degree in computer science from Allegheny College and a master's degree in computer science from the Stevens Institute of Technology. Prior to joining AWS, James was a senior infrastructure engineer at MITRE Corporation, a nonprofit government contractor, where he used his skills in infrastructure to help various govern-

ment organizations solve some of their toughest problems and realize the value of cloud computing.



**Alan Halachmi**, Senior Manager, Solutions Architecture, Amazon Web Services

Alan leads a team of specialist solutions architects supporting public sector customers. These specialists provide deep expertise in domains such as Geospatial Information Systems (GIS), High Performance Computing (HPC), and machine learning. Alan supports public sector organizations across the globe in the areas of networking and security. He holds a Certified Information Systems Security Professional (CISSP®)

certification as well as a half-dozen AWS certifications. He participated in the development of the Solutions Architect – Associate, Solutions Architect – Professional, and Advanced Networking – Specialty exams. Additionally, Alan has authored multiple AWS whitepapers that focus on the intersection of networking and security. Prior to joining Amazon, he worked in various leadership positions focused on homeland protection and identity systems at both established and startup companies in the private sector. Alan holds a bachelor's degree in network communication and information security from Duke University. In his free time, Alan enjoys family and tinkering with new toys.



**Matt Lehwess,** Principal Solutions Architect, Amazon Web Services

Matt has spent many years working as a network engineer in the network service provider space, building large-scale WAN networks in the Asia Pacific region and North America, as well as deploying data center technologies and their related network infrastructure. As a result, he is most at home working with Amazon VPC, AWS Direct Connect, and Amazon's other infrastructure-focused products and services. Matt is also a public speaker for AWS, and he enjoys spending time helping customers solve large-scale problems using the AWS Cloud platform. Outside of work, Matt is an avid rock climber, both indoor and outdoor, and a keen surfer. When he misses the waves of his hometown back in Australia, a trip to Santa Cruz, California from his home in San Francisco soon alleviates any homesick feelings.



**Nick Matthews,** Senior Solutions Architect, Amazon Web Services

Nick Matthews leads the networking segment of AWS partner support organization. He helps AWS partners create new networking solutions and make traditional networking products work on AWS. He enjoys assisting AWS customers to architect their networks for scalability and security. Nick also speaks at industry events on networking and security best practices. Before joining Amazon, Nick spent 10 years at Cisco working on Voice over IP (VoIP), Software-Defined Networking (SDN), and routing (Cisco Certified Internetwork Expert [CCIE] #23560). He founded the Network Programmability Users Group ([npug.net](http://npug.net)) to help users with SDN and programming network equipment. In his free time, he enjoys eating, drinking, and playing beach volleyball.



**Steve Morad,** Senior Manager, Solutions Builders, Amazon Web Services

Steve Morad holds a BA in computer science from Wheaton College (IL), and an MBA from Virginia Tech. He started his career by graduating from college and running off to join the circus. Since then, he gained systems administration, development, and architecture experience in the entertainment, financial services, and technology industries. Steve spent five years as a principal solutions architect supporting customers of all sizes and maturity levels, with a sub-specialty in AWS networking and security. He helped develop the Solutions Architect Associate, Developer Associate, SysOps Associate, Solutions Architect Professional, DevOps Professional, and Network Specialty exams. Steve is also an AWS public speaker and has developed network-related technical articles, whitepapers, and reference implementations. Steve is currently a senior manager of solutions builders at AWS. Outside of work, Steve enjoys helping coach soccer goalies and watching his kids perform in various musical ensembles.



**Steve Seymour,** Principal Solutions Architect, Amazon Web Services

Steve is a principal solutions architect and networking specialist within the AWS team covering Europe, the Middle East, and Africa. He uses his networking expertise to help customers of all sizes—from fast growing startups to the world's largest enterprises—use AWS networking technologies to meet and exceed their business requirements. Steve has more than 15 years of experience working with enterprise infrastructure, data center implementations, and migration projects with complex IP communications requirements. He is passionate about applying this experience to a broad range of industries to support customer success on AWS. Steve enjoys the outdoors, regularly coaches canoeing, and goes geocaching whenever traveling.



# Contents at a Glance

<i>Foreword</i>	<i>xxxiii</i>
<i>Introduction</i>	<i>xxxvii</i>
<i>Assessment Test</i>	<i>xliv</i>
<b>Chapter 1</b>	Introduction to Advanced Networking 1
<b>Chapter 2</b>	Amazon Virtual Private Cloud (Amazon VPC) and Networking Fundamentals 15
<b>Chapter 3</b>	Advanced Amazon Virtual Private Cloud (Amazon VPC) 57
<b>Chapter 4</b>	Virtual Private Networks 93
<b>Chapter 5</b>	AWS Direct Connect 129
<b>Chapter 6</b>	Domain Name System and Load Balancing 155
<b>Chapter 7</b>	Amazon CloudFront 207
<b>Chapter 8</b>	Network Security 233
<b>Chapter 9</b>	Network Performance 273
<b>Chapter 10</b>	Automation 305
<b>Chapter 11</b>	Service Requirements 345
<b>Chapter 12</b>	Hybrid Architectures 363
<b>Chapter 13</b>	Network Troubleshooting 397
<b>Chapter 14</b>	Billing 419
<b>Chapter 15</b>	Risk and Compliance 435
<b>Chapter 16</b>	Scenarios and Reference Architectures 467
<b>Appendix</b>	Answers to Review Questions 485
<i>Index</i>	<i>501</i>





# Contents

*Foreword* *xxxiii*

*Introduction* *xxxvii*

*Assessment Test* *xliv*

## **Chapter 1 Introduction to Advanced Networking 1**

AWS Global Infrastructure	2
Regions	2
Availability Zones	3
Edge Locations	4
Amazon Virtual Private Cloud	4
VPC Mechanics	4
Services Outside Your VPC	5
AWS Networking Services	7
Amazon Elastic Compute Cloud	7
Amazon Virtual Private Cloud	7
AWS Direct Connect	7
Elastic Load Balancing	7
Amazon Route 53	8
Amazon CloudFront	8
GuardDuty	8
AWS WAF	8
AWS Shield	8
Summary	9
Resources to Review	9
Exam Essentials	10
Exercise	11
Review Questions	12

## **Chapter 2 Amazon Virtual Private Cloud (Amazon VPC) and Networking Fundamentals 15**

Introduction to Amazon Virtual Private Cloud (Amazon VPC)	16
Subnets	19
Route Tables	22
IP Addressing	23
IPv4 Addresses	24
IPv6 Addresses	25
Security Groups	26
Network Access Control Lists (ACLs)	29
Internet Gateways	30

Network Address Translation (NAT) Instances and NAT Gateways	31
NAT Instance	32
NAT Gateway	33
Egress-Only Internet Gateways (EIGWs)	33
Virtual Private Gateways (VGWs), Customer Gateways, and Virtual Private Networks (VPNs)	35
VPC Endpoints	36
VPC Peering	38
Placement Groups	40
Elastic Network Interfaces	41
Dynamic Host Configuration Protocol (DHCP) Option Sets	42
Amazon Domain Name Service (DNS) Server	43
VPC Flow Logs	43
Summary	45
Resources to Review	48
Exam Essentials	48
Exercises	51
Review Questions	55
 <b>Chapter 3</b>	
<b>Advanced Amazon Virtual Private Cloud (Amazon VPC)</b>	<b>57</b>
VPC Endpoints	58
VPC Endpoints and Security	59
VPC Endpoint Policy	59
VPC Endpoint Overview	59
Gateway VPC Endpoints	59
Interface VPC Endpoints	60
AWS PrivateLink	60
Gateway VPC Endpoints	60
Amazon S3 Endpoints	60
Amazon DynamoDB Endpoints	62
Accessing Gateway Endpoints Over Remote Networks	62
Securing Gateway VPC Endpoints	63
Interface VPC Endpoints	64
Interface VPC Endpoints	64
AWS PrivateLink for Customer and Partner Services	65
Comparing AWS PrivateLink and VPC Peering	67
AWS PrivateLink Service Provider Considerations	68
AWS PrivateLink Service Consumer Considerations	68
Accessing a Shared Services VPC	69

Transitive Routing	70
Routing Across Peered VPCs	73
IP Addressing Features	74
Resizing a VPC	74
Resizing VPC Considerations	74
IP Address Features	76
Reclaiming Elastic IP Addresses	76
Cross-Account Network Interfaces	76
Design Considerations	76
Comparison with VPC Peering and VPC Endpoints	77
Summary	77
Exam Essentials	78
Resources to Review	80
Exercises	80
Review Questions	88
 <b>Chapter 4</b>	 <b>Virtual Private Networks</b>
	<b>93</b>
Introduction to Virtual Private Networks	94
Site-to-Site VPN	94
Virtual Private Gateway as a VPN Termination Endpoint	95
Availability and Redundancy	96
VPN Features	97
AWS VPN CloudHub	98
VPN Creation Process	100
Monitoring	101
Amazon Elastic Compute Cloud (Amazon EC2)	
Instance as a VPN Termination Endpoint	101
Availability and Redundancy	102
Amazon EC2 Features	104
VPN Creation Process	104
Monitoring	106
Performance	106
VPN Termination Endpoint for On-Premises	
Networks (Customer Gateways)	110
Third-Party VPN Device	111
Client-to-Site VPN	112
Design Patterns	114
Summary	117
Exam Essentials	119
Resources to Review	120
Exercises	121
Review Questions	126

<b>Chapter 5</b>	<b>AWS Direct Connect</b>	<b>129</b>
	What Is AWS Direct Connect?	130
	Core Concepts	130
	802.1Q Virtual Local Area Networks (VLANs)	130
	Border Gateway Protocol	130
	Bidirectional Forwarding Detection	131
	Physical Connectivity	131
	AWS Direct Connect Locations	131
	Dedicated Connections	131
	Provisioning Process	132
	Requesting a Connection	132
	Download Your Letter of Authorization	132
	Cross-Connect to the AWS Port	132
	Multiple Connections	133
	Link Aggregation Groups	134
	AWS Direct Connect Partners	134
	Hosted Connections	135
	Logical Connectivity	135
	Virtual Interfaces	136
	Public Virtual Interfaces	137
	Private Virtual Interfaces	138
	Direct Connect Gateway	139
	Hosted Virtual Interfaces	140
	Resilient Connectivity	140
	Single Connection	140
	Dual Connection: Single Location	140
	Single Connections: Dual Locations	141
	Dual Connections: Dual Locations	143
	Virtual Interface Configuration	143
	Public Virtual Interface Configuration	143
	Private Virtual Interface Configuration	143
	Bidirectional Forwarding Detection	144
	Virtual Private Network with AWS Direct Connect	144
	Backup Virtual Private Network (VPN)	144
	Virtual Private Network Over AWS Direct Connect	145
	Integration with the Transit Virtual Private	
	Cloud Solution	146
	Border Gateway Protocol Path Selection	147
	Billing	147
	Port-Hours	147
	Data Transfer	148
	Private Virtual Interface Data Transfer	148
	Public Virtual Interface Data Transfer	148

Summary	149
Exam Essentials	149
Resources to Review	150
Exercises	150
Review Questions	153
<b>Chapter 6</b>	<b>Domain Name System and Load Balancing</b>
	<b>155</b>
Introduction to Domain Name System and Load Balancing	156
Domain Name System	156
Domain Name System Concepts	157
Top-Level Domains	157
Domain Names, Subdomains, and Hosts	158
IP Addresses	158
Fully Qualified Domain Names	158
Name Servers	159
Zones	159
Domain Name Registrars	159
Steps Involved in DNS Resolution	160
TLD Servers	160
Domain Level Name Servers	160
Resolving Name Servers	161
Record Types	161
Start of Authority Record	161
A and AAAA	162
Certificate Authority Authorization	162
Canonical Name	162
Mail Exchange	162
Name Authority Pointer	162
Name Server	162
Pointer	162
Sender Policy Framework	163
Text	163
Service	163
Amazon EC2 DNS Service	163
Amazon EC2 DNS vs. Amazon Route 53	165
Amazon EC2 DNS and VPC Peering	165
Using DNS with Simple AD	166
Custom Amazon EC2 DNS Resolver	166
Amazon Route 53	168
Domain Registration	169
Transferring Domains	170
Domain Name System Service	171
Hosted Zones	172

Supported Record Types	172
Routing Policies	173
Simple Routing Policy	173
Weighted Routing Policy	173
Latency-Based Routing Policy	174
Failover Routing Policy	174
Geolocation Routing Policy	175
Multivalue Answer Routing	176
Traffic Flow to Route DNS Traffic	177
Geoproximity Routing (Traffic Flow Only)	177
More on Health Checking	178
Elastic Load Balancing	180
Types of Load Balancers	181
Classic Load Balancer	183
Application Load Balancer	184
Network Load Balancer	184
Internet-Facing Load Balancers	186
Internal Load Balancers	187
HTTPS Load Balancers	187
Elastic Load Balancing Concepts	187
Listeners	187
Listener Rules	188
Targets	188
Target Groups	189
Elastic Load Balancer Configuration	189
Idle Connection Timeout	189
Cross-Zone Load Balancing	190
Connection Draining (Deregistration Delay)	190
Proxy Protocol	190
Sticky Sessions	191
Health Checks	191
ELB Sandwich	192
Summary	193
Exam Essentials	196
Resources to Review	198
Exercises	199
Review Questions	205

<b>Chapter 7</b>	<b>Amazon CloudFront</b>	<b>207</b>
	Introduction to Amazon CloudFront	208
	Content Delivery Network Overview	208
	The AWS CDN: Amazon CloudFront	209
	Amazon CloudFront Basics	209
	Distributions	209
	Origins	210
	Cache Control	210

How Amazon CloudFront Delivers Content	210
Configuring Amazon CloudFront	211
How CloudFront Operates	212
Amazon CloudFront Edge Locations	214
Amazon CloudFront Regional Edge Caches	214
Web Distributions	215
Dynamic Content and Advanced Features	215
Dynamic Content, Multiple Origins, and Cache Behaviors	215
A Note on Performance: Dynamic Content and HTTP/2	216
Whole Website	217
Private Content	217
RTMP Distributions	218
Alternate Domain Names	219
HTTPS	220
Amazon CloudFront and AWS Certificate Manager (ACM)	221
Invalidating Objects (Web Distributions Only)	221
Access Logs	222
Amazon CloudFront and AWS Lambda@Edge	222
Amazon CloudFront Field-Level Encryption	223
Summary	224
Exam Essentials	224
Resources to Review	225
Exercises	226
Review Questions	230

## **Chapter 8      Network Security      233**

Governance	235
AWS Organizations	235
AWS CloudFormation	236
AWS Service Catalog	237
Data Flow Security	238
Edge Locations	238
Amazon Route 53	238
Amazon CloudFront	240
AWS Lambda@Edge	241
Edge Locations and Regions	242
AWS Certificate Manager	242
AWS WAF	242
AWS Shield	245

Regions	246
Elastic Load Balancing	246
Subnets and Route Tables	247
Security Groups and Network Access Control Lists (ACLs)	249
Amazon Elastic Compute Cloud (Amazon EC2)	250
Regional Services	252
AWS Security Services	252
Amazon GuardDuty	252
Amazon Inspector	253
Amazon Macie	253
Detection and Response	254
Secure Shell (SSH) Login Attempts	254
AWS Cloud Services	254
Architecture Overview	255
Solution Description	255
Network Traffic Analysis	256
AWS Cloud Services	256
Architecture Overview	257
Solution Description	257
IP Reputation	258
AWS Cloud Services	258
Architecture Overview	259
Solution Description	259
Summary	260
Resources to Review	262
Exam Essentials	264
Exercises	266
Review Questions	269

## **Chapter 9      Network Performance      273**

Network Performance Basics	274
Bandwidth	274
Latency	275
Jitter	275
Throughput	275
Packet Loss	275
Packets per Second	276
Maximum Transmission Unit	276
Amazon Elastic Compute Cloud (Amazon EC2) Instance	
Networking Features	276
Instance Networking	276
Placement Groups	277
Amazon Elastic Block Store (Amazon EBS)-Optimized Instances	277
Network Address Translation (NAT) Gateways	278



Enhanced Networking	278
Network Drivers	278
Enabling Enhanced Networking	279
Operating System Support	279
Additional Tuning and Driver Support	279
Optimizing Performance	279
Enhanced Networking	280
Jumbo Frames	280
Network Credits	280
Instance Bandwidth	281
Flow Performance	281
Load Balancer Performance	281
Virtual Private Network (VPN) Performance	282
AWS Direct Connect Performance	282
Quality of Service (QoS) in a VPC	282
Example Applications	283
High Performance Computing	283
Real-Time Media	283
Data Processing, Ingestion, and Backup	284
On-Premises Data Transfer	284
Network Appliances	285
Performance Testing	286
Amazon CloudWatch Metrics	286
Testing Methodology	288
Throughput Testing	288
Solution Testing	289
Summary	289
Resources to Review	290
Exam Essentials	290
Exercises	292
Review Questions	299

## **Chapter 10      Automation      305**

Introduction to Network Automation	306
Infrastructure as Code	306
Templates and Stacks	307
Stack Dependencies	310
Errors and Rollbacks	314
Template Parameters	315
Verifying Changes with Change Sets	318
Retaining Resources	319
Configuring Non-AWS Resources	319
Security Best Practices	321
Configuration Management	322

	Continuous Delivery	322
	Pipeline Stages, Actions, and Artifacts	323
	Approvals	323
	Network Monitoring Tools	325
	Monitoring Network Health Metrics	325
	Creating Alarms for Unusual Events	327
	Collecting Text Logs	329
	Converting Logs to Metrics	330
	Summary	331
	Exam Essentials	331
	Resources to Review	333
	Exercises	334
	Review Questions	341
<b>Chapter 11</b>	<b>Service Requirements</b>	<b>345</b>
	Introduction to Service Requirements	346
	The Elastic Network Interface	346
	AWS Cloud Services and Their Network Requirements	346
	Amazon WorkSpaces	346
	Amazon WorkSpaces Requirements	347
	Amazon AppStream 2.0	347
	Amazon AppStream 2.0 Requirements	348
	AWS Lambda (Within a VPC)	348
	AWS Lambda Requirements	348
	Amazon EC2 Container Service (Amazon ECS)	349
	Amazon ECS Requirements	350
	Amazon EMR	350
	Amazon EMR Requirements	350
	Amazon Relational Database Service (Amazon RDS)	351
	Amazon RDS Requirements	351
	AWS Database Migration Service (AWS DMS)	351
	AWS DMS Requirements	352
	Amazon Redshift	352
	Amazon Redshift Requirements	352
	AWS Glue	353
	AWS Glue Requirements	353
	AWS Elastic Beanstalk	353
	AWS Elastic Beanstalk Requirements	354
	Summary	354
	Exam Essentials	355
	Resources to Review	356
	Exercises	357
	Review Questions	360

<b>Chapter 12</b>	<b>Hybrid Architectures</b>	<b>363</b>
	Introduction to Hybrid Architectures	364
	Choices for Connectivity	364
	Application Architectures	365
	Three-Tier Web Application	365
	Active Directory	367
	Domain Name System (DNS)	368
	Applications Requiring Consistent Network Performance	368
	Hybrid Operations	370
	Remote Desktop Application: Amazon Workspaces	371
	Application Storage Access	371
	Amazon Simple Storage Service (Amazon S3)	372
	Amazon Elastic File System (Amazon EFS)	374
	Hybrid Cloud Storage: AWS Storage Gateway	374
	Application Internet Access	375
	Access VPC Endpoints and	
	Customer-Hosted Endpoints over	
	AWS Direct Connect	375
	Encryption on AWS Direct Connect	376
	Use of Transitive Routing in Hybrid IT	379
	Transit VPC Architecture Considerations	380
	Transit VPC Scenarios	384
	Summary	386
	Exam Essentials	388
	Resources to Review	389
	Exercises	389
	Review Questions	394
 <b>Chapter 13</b>	 <b>Network Troubleshooting</b>	 <b>397</b>
	Introduction to Network Troubleshooting	398
	Methodology for Troubleshooting	398
	Network Troubleshooting Tools	399
	Traditional Tools	399
	Packet Captures	399
	ping	399
	tracert	399
	Telnet	399
	nslookup	399
	AWS-Native Tools	400
	Amazon CloudWatch	400
	Amazon VPC Flow Logs	401
	AWS Config	401
	AWS Trusted Advisor	401
	AWS Identity and Access Management (IAM)	
	Policy Simulator	401

Troubleshooting Common Scenarios	401
Internet Connectivity	402
Virtual Private Network	402
Internet Key Exchange (IKE) Phase 1 and Phase 2 Troubleshooting	403
AWS Direct Connect	404
Security Groups	404
Network Access Control Lists	405
Routing	405
Virtual Private Cloud (VPC) Peering Connections	406
Connectivity to AWS Cloud Services	407
Amazon CloudFront Connectivity	407
Elastic Load Balancing Functionality	408
Domain Name System	408
Hitting Service Limits	409
Summary	409
Exam Essentials	410
Resources to Review	411
Exercises	412
Review Questions	415
 <b>Chapter 14</b>	 <b>Billing</b>
	<b>419</b>
Billing Overview	420
Service and Port-Hour Fees	420
Virtual Private Network (VPN) Connections	420
AWS Direct Connect	421
AWS PrivateLink	421
NAT Gateway	421
Elastic Load Balancing	421
Types of Data Transfer	422
Data Transfer: Internet	423
Data Transfer: Region to Region	423
Amazon CloudFront	423
Data Transfer: Same Region via Public IP	423
Data Transfer: Inter-Availability Zone	423
Data Transfer: VPC Peering	424
Data Transfer: Intra-Availability Zone	424
Virtual Private Network (VPN) Endpoints (Virtual Private Gateways [VGWs])	424
AWS Direct Connect Public Virtual Interfaces (VIFs)	424
Scenarios	424
Scenario 1	424
Scenario 2	424
Scenario 3	426

	Scenario 4	426
	Scenario 5	426
	Scenario 6	428
	Summary	428
	Exam Essentials	428
	Resources to Review	429
	Exercises	429
	Review Questions	432
<b>Chapter 15</b>	<b>Risk and Compliance</b>	<b>435</b>
	It All Begins with Threat Modeling	436
	Compliance and Scoping	437
	Audit Reports and Other Papers	438
	Ownership Model and the Role of Network Management	439
	Controlling Access to AWS	439
	AWS Organizations	441
	Amazon CloudFront Distributions	441
	Encryption Options	442
	AWS API Calls and Internet API Endpoints	442
	Selecting Cipher Suites	443
	Encryption in Transit Inside AWS Environments	443
	Encryption in Load Balancers and Amazon	
	CloudFront PoPs	444
	Network Activity Monitoring	444
	AWS CloudTrail	445
	AWS Config	445
	Amazon CloudWatch	446
	Amazon CloudWatch Logs	447
	Amazon VPC Flow Logs	448
	Amazon CloudFront	449
	Other Log Sources	449
	Malicious Activity Detection	449
	AWS Shield and Anti-DDoS Measures	449
	Amazon VPC Flow Logs Analysis	451
	Amazon CloudWatch Alerting and AWS Lambda	452
	AWS Marketplace and Other Third-Party Offerings	452
	Security Information and Event Management (SIEM)	452
	Intrusion Detection System (IDS)/Intrusion	
	Prevention System (IPS)/AWS Web Application	
	Firewall (AWS WAF)	452
	Amazon Inspector	453
	Other Compliance Tools	453

	Penetration Testing and Vulnerability Assessment	454
	Penetration Test Authorization Scope and Exceptions	454
	Applying for and Receiving Penetration Test Authorization	455
	Summary	456
	Exam Essentials	457
	Resources to Review	458
	Exercises	459
	Review Questions	464
<b>Chapter 16</b>	<b>Scenarios and Reference Architectures</b>	<b>467</b>
	Introduction to Scenarios and Reference Architectures	468
	Hybrid Networking Scenario	468
	Multi-Location Resiliency	472
	Summary	476
	Resources to Review	476
	Exam Essentials	477
	Exercises	478
	Review Questions	481
<b>Appendix</b>	<b>Answers to Review Questions</b>	<b>485</b>
	Chapter 1: Introduction to Advanced Networking	486
	Chapter 2: Amazon Virtual Private Cloud (Amazon VPC) and Networking Fundamentals	487
	Chapter 3: Advanced Amazon Virtual Private Cloud (Amazon VPC)	487
	Chapter 4: Virtual Private Networks	489
	Chapter 5: AWS Direct Connect	490
	Chapter 6: Domain Name System and Load Balancing	490
	Chapter 7: Amazon CloudFront	491
	Chapter 8: Network Security	492
	Chapter 9: Network Performance	493
	Chapter 10: Automation	495
	Chapter 11: Service Requirements	496
	Chapter 12: Hybrid Architectures	497
	Chapter 13: Network Troubleshooting	498
	Chapter 14: Billing	498
	Chapter 15: Risk and Compliance	499
	Chapter 16: Scenarios and Reference Architectures	499
	<i>Index</i>	501