

ANTHONY SEQUEIRA

Cert Guide

Learn, prepare, and practice for exam success



AWS Certified Cloud Practitioner Exam

Rough Cuts

PEARSON IT
CERTIFICATION

Save 10%
on Exam
Voucher

See Inside

AWS Certified Cloud Practitioner (CLF-C01) Cert Guide

Anthony Sequeira, CCIE #15626

Pearson IT Certification

AWS Certified Cloud Practitioner (CLF-C01) Cert Guide

Copyright © 2019 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-10: 0-78976-048-7

ISBN-13: 978-0-78976-048-7

Library of Congress Control Number: 2019930941

First Printing: April 2019

1 19

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

This book is designed to provide information about the AWS Certified Cloud Practitioner exam. Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the supplemental online content or programs accompanying it.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Editor-in-Chief: Mark Taub

Product Line Manager: Brett Bartow

Acquisitions Editor: Paul Carlstroem

Managing Editor: Sandra Schroeder

Development Editor: Christopher Cleveland

Project Editor: Mandie Frank

Copy Editor: Bart Reed

Technical Editor: Ryan Dymek

Editorial Assistant: Cindy Teeters

Designer: Chuti Prasertsith

Composition:

Indexer:

Contents at a Glance

Introduction

Part I Domain 1: Cloud Concepts

Chapter 1 The AWS Cloud Defined

Chapter 2 Advantages of the AWS Cloud

Chapter 3 Core AWS Services

Chapter 4 Cloud Architecture Design Principles

Part II Domain 2: Security

Chapter 5 The AWS Shared Responsibility Model

Chapter 6 Cloud Security and Compliance

Chapter 7 AWS Access Management Capabilities

Chapter 8 Resources for Security Support

Part III Domain 3: Technology

Chapter 9 Methods of Deploying and Operating in AWS

Chapter 10 The AWS Global Infrastructure

Chapter 11 Resources for Technology Support

Part IV Domain 4: Billing and Pricing

Chapter 12 Using the Free Tier to Build a Web Server

Chapter 13 AWS Pricing Models

Chapter 14 Account Structures for Billing and Pricing

Chapter 15 Resources for Billing Support

Part V Final Preparation

Chapter 16 Final Preparation

Part VI Appendixes

Glossary of Key Terms

Appendix A Answers to the “Do I Know This Already?”
Quizzes and Q&A Sections

Appendix B AWS Certified Cloud Practitioner (CLF-C01)
Exam Updates

Appendix C Study Planner

Table of Contents

About the Author

Dedication

Acknowledgments

About the Technical Reviewer

We Want to Hear from You!

Reader Services

Introduction

The Goals of the AWS Certified Cloud Practitioner Program

The Exam Objectives (Domains)

Steps to Becoming an AWS Certified Cloud Practitioner

Facts About the Exam

How to Use this Book

Companion Website

Pearson Test Prep Practice Test Software

Accessing the Pearson Test Prep Software Online

Accessing the Pearson Test Prep Software Offline

Customizing Your Exams

Updating Your Exams

Part I. Domain 1: Cloud Concepts

Chapter 1. The AWS Cloud Defined

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[Introduction to the Cloud](#)

[Introduction to the AWS Cloud](#)

[Exam Preparation Tasks](#)

[Q&A](#)

Chapter 2. Advantages of the AWS Cloud

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[Cloud Advantages](#)

[AWS Cloud Advantages](#)

[Exam Preparation Tasks](#)

[Q&A](#)

Chapter 3. Core AWS Services

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[Overview of Services and Categories](#)

[Introduction to the AWS Global Infrastructure](#)

[Introduction to Virtual Private Cloud](#)

[Introduction to Security Groups](#)

[Introduction to Compute Services](#)

[Introduction to EBS](#)

[Introduction to S3](#)

[Introduction to AWS Database Solutions](#)

[Exam Preparation Tasks](#)

[Q&A](#)

[Chapter 4. Cloud Architecture Design Principles](#)

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[The Well-Architected Framework](#)

[Fault Tolerance and High Availability](#)

[Web Hosting](#)

[Exam Preparation Tasks](#)

[Q&A](#)

[Part II. Domain 2: Security](#)

[Chapter 5. The AWS Shared Responsibility Model](#)

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[Understanding the Shared Responsibility Model](#)

[Amazon Responsibilities](#)

[Client Responsibilities](#)

[Exam Preparation Tasks](#)

[Q&A](#)

[Chapter 6. Cloud Security and Compliance](#)

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[An Introduction to AWS Security](#)

[AWS Security Compliance Programs](#)

[Exam Preparation Tasks](#)

[Q&A](#)

[Chapter 7. AWS Access Management Capabilities](#)

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[Identity and Access Management](#)

[Best Practices with IAM](#)

[Exam Preparation Tasks](#)

[Q&A](#)

[Chapter 8. Resources for Security Support](#)

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[Tools for Security Support](#)

[Additional Security Support Resources](#)

[Exam Preparation Tasks](#)

[Q&A](#)

Part III. Domain 3: Technology

Chapter 9. Methods of Deploying and Operating in AWS

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[Automation](#)

[Orchestration](#)

[Management Options](#)

[Exam Preparation Tasks](#)

[Q&A](#)

Chapter 10. The AWS Global Infrastructure

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[Regions](#)

[Availability Zones](#)

[Connections](#)

[Exam Preparation Tasks](#)

[Q&A](#)

Chapter 11. Resources for Technology Support

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[Documentation](#)

[Discussion Forums](#)

[Exam Preparation Tasks](#)

[Q&A](#)

[Part IV. Domain 4: Billing and Pricing](#)

[Chapter 12. Using the Free Tier to Build a Web Server](#)

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[Creating Your Free Tier Account](#)

[Exam Preparation Tasks](#)

[Q&A](#)

[Chapter 13. AWS Pricing Models](#)

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[Fundamentals of Pricing](#)

[Pricing Details](#)

[Exam Preparation Tasks](#)

[Q&A](#)

[Chapter 14. Account Structures for Billing and Pricing](#)

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[AWS Support Plans Overview](#)

[Comparing the Plans](#)

[Exam Preparation Tasks](#)

[Q&A](#)

[Chapter 15. Resources for Billing Support](#)

[“Do I Know This Already?” Quiz](#)

[Foundation Topics](#)

[Cost Calculators](#)

[AWS Billing and Cost Management](#)

[Exam Preparation Tasks](#)

[Q&A](#)

[Part V. Final Preparation](#)

[Chapter 16. Final Preparation](#)

[Exam Information](#)

[Getting Ready](#)

[Tools for Final Preparation](#)

[Suggested Plan for Final Review/Study](#)

[Summary](#)

[Part VI. Appendixes](#)

[Glossary of Key Terms](#)

[Appendix A. Answers to the “Do I Know This Already?”](#)

[Quizzes and Q&A Sections](#)

[Do I Know This Already? Answers](#)

[Q&A Answers](#)

Appendix B. AWS Certified Cloud Practitioner (CLF-C01) Cert Guide Exam Updates

Always Get the Latest at the Book's Product Page

Technical Content

Appendix C. Study Planner [This content is currently in development.]

About the Author

Anthony Sequeira, CCIE No. 15626, is a seasoned trainer and author regarding various levels and tracks of Cisco, Microsoft, and AWS certifications. Anthony formally began his career in the information technology industry in 1994 with IBM in Tampa, Florida. He quickly formed his own computer consultancy, Computer Solutions, and then discovered his true passion—teaching and writing about information technologies.

Anthony joined Mastering Computers in 1996 and lectured to massive audiences around the world about the latest in computer technologies. Mastering Computers became the revolutionary online training company, KnowledgeNet, and Anthony trained there for many years.

Anthony is currently pursuing his second CCIE in the area of Cisco Data Center! Anthony is a full-time instructor at CBT Nuggets.

Dedication

I would like to dedicate this book to the many students I have encountered in the last 25 years of my career. You have kept me learning and teaching to the very best of my abilities.

Thank you!

Acknowledgments

This manuscript was made truly great by the incredible technical review of Ryan Dymek. Sometimes I think he might have invented AWS.

I would also like to express my gratitude to Chris Cleveland, development editor of this book. I was so incredibly lucky to work with him again on this text. Like Ryan, he made this book several cuts above the rest.

About the Technical Reviewer

Ryan Dymek

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email: community@informit.com

Reader Services

Register your copy of *AWS Certified Cloud Practitioner (CLF-C01) Cert Guide* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789760487 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

*Be sure to check the box that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

The Cloud Practitioner exam provides individuals with an overall understanding of the AWS Cloud to validate their knowledge with an industry-recognized credential. This exam provides individuals in a larger variety of cloud and technology roles with a way to validate their AWS Cloud knowledge and enhance their professional credibility. This exam covers four domains: Cloud Concepts, Security, Technology, and Billing and Pricing. The AWS Certified Cloud Practitioner is a recommended path to achieving further specialty certifications or an optional start toward associate certifications in various disciplines such as solutions architect, SysOps administrator, and developer.

THE GOALS OF THE AWS CERTIFIED CLOUD PRACTITIONER PROGRAM

After a candidate studies this text carefully, they should be more than ready for their certification exam. Perhaps more importantly, however, these candidates should possess the following abilities:

- To define what is meant by the AWS Cloud
- To describe the basics of the AWS Global Infrastructure
- To describe basic AWS Cloud architecture principles

- To describe the value propositions of using AWS Cloud technologies
- To describe the key services of the AWS platform and the categories these services fall under
- To describe the AWS shared responsibility model
- To describe the basic security and compliance capabilities within AWS
- To define the billing, account management, and pricing models within AWS
- To identify sources of documentation and support for technical assistance
- To describe the basics of deploying and operating technologies in the AWS Cloud

Ideal Candidates

While this text provides you with the information required to pass this exam, Amazon considers ideal candidates to be those that possess the following:

- Six months of experience with the AWS Cloud in any role, including technical, managerial, sales, purchasing, or financial
- A basic understanding of IT services and their uses in the AWS Cloud platform

THE EXAM OBJECTIVES (DOMAINS)

The AWS Certified Cloud Practitioner (CLF-C01) exam is broken down into four major domains. The contents of this book cover each of the domains and the subtopics included in them, as illustrated in the following descriptions.

The following table lists the breakdown of each of the domains represented in the exam.

Domain	Percentage of Representation in Exam
1: Cloud Concepts	28%
2: Security	24%
3: Technology	36%
4: Billing and Pricing	12%
	Total 100%

1.0 Cloud Concepts

The Cloud Concepts domain is covered in Chapters 1 through 4. It covers critical topics such as the services and categories of services provided by AWS. This domain also covers important information on just how AWS can save your IT team large sums of money. It comprises 28% of the exam and includes the following topics:

- 1.1 Define the AWS Cloud and its value proposition
- 1.2 Identify aspects of AWS Cloud economics
- 1.3 List the different cloud architecture design principles

2.0 Security

The Security domain is covered in Chapters 5 through 8. This domain covers security in general with AWS, but also provides details on the implementation of strong security with such AWS services as IAM and a wide variety of management tools. This domain makes up 24% of the exam and includes the following topics:

- 2.1 Define the AWS Shared Responsibility model
- 2.2 Define AWS Cloud security and compliance concepts
- 2.3 Identify AWS access management capabilities
- 2.4 Identify resources for security support

3.0 Technology

The Technology domain is covered in Chapters 9 through 11. This domain digs in to the “nuts and bolts” of AWS. The global infrastructure and core services of AWS are all detailed for you. It encompasses 36% of the exam and includes the following topics:

- 3.1 Define methods of deploying and operating in the AWS Cloud
- 3.2 Define the AWS global infrastructure
- 3.3 Identify the core AWS services
- 3.4 Identify resources for technology support

4.0 Billing and Pricing

The Billing and Pricing domain is covered in Chapters 12 through 15. Here, you learn of the tools and techniques for controlling costs inside of AWS as well as the resources that are available to assist you. This domain embodies 12% of the exam and includes the following topics:

- 4.1 Compare and contrast the various pricing models for AWS
- 4.2 Recognize the various account structures in relation to AWS billing and pricing
- 4.3 Identify resources available for billing support

STEPS TO BECOMING AN AWS CERTIFIED CLOUD PRACTITIONER

To become an AWS Certified Cloud Practitioner, a test candidate should meet certain prerequisites and follow specific procedures. Once they deem themselves ready, test candidates must sign up for the exam.

Signing Up for the Exam

The steps required to sign up for the AWS Certified Cloud Practitioner are as follows:

1. Create an AWS Certification account at <https://www.aws.training/Certification> and schedule your exam.

2. Complete the Examination Agreement, attesting to the truth of your assertions regarding professional experience and legally committing to the adherence of the testing policies.
3. Submit the examination fee.

FACTS ABOUT THE EXAM

The exam is a computer-based test. The exam consists of multiple-choice questions only. You must bring a government-issued identification card. No other forms of ID will be accepted.

Tip

Refer to the AWS Certification site at <https://aws.amazon.com/certification/> for more information regarding this, and other, AWS certifications. I am also in the process of building a simple hub site for everything AWS certification related at awscerthub.com. This site is made up of 100% AWS solutions, of course!

HOW TO USE THIS BOOK

This book maps directly to the topic areas of the exam and uses a number of features to help you understand the topics and prepare for the exam.

Objectives and Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to

help you prove to yourself that you have retained your knowledge of those topics. This book does not try to help you pass the exam only by memorization; it seeks to help you to truly learn and understand the topics. This book is designed to help you pass the AWS Certified Cloud Practitioner exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the companion website

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **Foundation Topics:** These are the core sections of each chapter. They explain the concepts for the topics in that chapter.
- **Exam Preparation Tasks:** After the “Foundation Topics” section of each chapter, the “Exam Preparation Tasks” section lists a series of study activities that you should do at the end of the chapter:

- **Review All Key Topics:** The Key Topic icon appears next to the most important items in the “Foundation Topics” section of the chapter. The “Review All Key Topics” activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.
- **Define Key Terms:** Although the Cloud Practitioner exam may be unlikely to ask a question such as “Define this term,” the exam does require that you learn and know a lot of AWS-related terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the Glossary at the end of the book.
- **Q&A Questions:** Confirm that you understand the content you just covered by answering these questions and reading the answer explanations.
- **Web-based practice exam:** The companion website includes the Pearson Cert Practice Test engine, which allows you to take practice exam questions. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

How This Book Is Organized

This book contains 15 core chapters—Chapters 1 through 15. Chapter 16 includes preparation tips and suggestions for how to approach the exam. The core chapters map to the AWS

Certified Cloud Practitioner exam topic areas and cover the concepts and technologies you will encounter on the exam.

COMPANION WEBSITE

Register this book to get access to the Pearson IT Certification test engine and other study materials, plus additional bonus content. Check this site regularly for new and updated postings written by the authors that provide further insight into the more troublesome topics on the exam. Be sure to check the box that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

Step 1. Go to www.pearsonitcertification.com/register and log in or create a new account.

Step 2. Enter the ISBN: **9780789760487**.

Step 3. Answer the challenge question as proof of purchase.

Step 4. Click the **Access Bonus Content** link in the “Registered Products” section of your account page to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following the steps at left, please visit

www.pearsonITcertification.com/contact and select the **Site Problems/ Comments** option. Our customer service representatives will assist you.

PEARSON TEST PREP PRACTICE TEST SOFTWARE

As noted previously, this book comes complete with the Pearson Test Prep practice test software containing two full exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

ACCESSING THE PEARSON TEST PREP SOFTWARE ONLINE

The online version of this software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, simply follow these steps:

Step 1. Go to <https://www.PearsonTestPrep.com>.

Step 2. Select **Pearson IT Certification** as your product group.

Step 3. Enter your email/password for your account. If you don't have an account on PearsonITCertification.com

or CiscoPress.com, you will need to establish one by going to PearsonITCertification.com/join.

Step 4. In the **My Products** tab, click the **Activate New Product** button.

Step 5. Enter the access code printed on the insert card in the back of your book to activate your product.

Step 6. The product will now be listed in your “My Products” page. Click the **Exams** button to launch the exam settings screen and start your exam.

ACCESSING THE PEARSON TEST PREP SOFTWARE OFFLINE

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book’s companion website, or you can just enter this link in your browser:

<http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip>

To access the book’s companion website and the software, simply follow these steps:

Step 1. Register your book by going to PearsonITCertification.com/register and entering the ISBN: **9780789760487**.

Step 2. Answer the challenge questions.

- Step 3.** Go to your account page and click the **Registered Products** tab.
- Step 4.** Click the **Access Bonus Content** link under the product listing.
- Step 5.** Click the **Install Pearson Test Prep Desktop Version** link under the “Practice Exams” section of the page to download the software.
- Step 6.** After the software finishes downloading, unzip all the files on your computer.
- Step 7.** Double-click the application file to start the installation, and follow the onscreen instructions to complete the registration.
- Step 8.** After the installation is complete, launch the application and click the **Activate Exam** button on the **My Products** tab.
- Step 9.** Click the **Activate a Product** button in the Activate Product Wizard.
- Step 10.** Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.
- Step 11.** Click **Next** and then click **Finish** to download the exam data to your application.
- Step 12.** Start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions will synch together, so saved exams and grade results recorded on one version will be available to you on the other as well.

CUSTOMIZING YOUR EXAMS

Once you are in the exam settings screen, you can choose to take exams in one of three modes:

- **Study mode:** Allows you to fully customize your exam and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness.
- **Flash Card mode:** Strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes do, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters or you can narrow your selection to just a single chapter or the chapters that make up a specific

part in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the “Objectives” area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you as well as two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions for which you have added notes.

UPDATING YOUR EXAMS

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software while connected to the Internet, it checks if there are any updates to your exam data and automatically downloads any

changes that were made since the last time you used the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams. To update a particular exam you have already activated and downloaded, simply click the **Tools** tab and click the **Update Products** button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply click the **Tools** tab and click the **Update Application** button. This ensures you are running the latest version of the software engine.

Part I

Domain 1: Cloud Concepts

Chapter 1

The AWS Cloud Defined

This chapter covers the following subjects:

- **Introduction to the Cloud:** You might have heard of cloud technologies before. This is, of course, a bit of a joke since cloud is one of the hottest topics in Information Technology—and not surprisingly, one of the most significant areas of demand in tech employment. This section of the chapter introduces you to the cloud technologies and details why they are so important and exciting.
- **Introduction to the AWS Cloud:** This section of the chapter provides an overview of crucial service categories and services themselves. While these services are given greater detail later in this book, this early look is critical for you to start building your AWS understanding and vocabulary.

In this critical chapter, we talk about the various characteristics of technology that would qualify a solution as “cloud.” This chapter, as you might guess, also examines the specifics of Amazon Web Services (AWS) that help to make it the most popular (by far) public cloud offering.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. [Table 1-1](#) lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 1-1 “Do I Know This Already?” Foundation Topics
Section-to-Question Mapping

Foundations Topics Section	Questions
Introduction to the Cloud	1–3
Introduction to the AWS Cloud	4–6

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following is not a common cloud characteristic as defined by the NIST?
 - a. On-demand self-service

- b.** Measured service
 - c.** Broad network access
 - d.** Dedicated hardware
- 2.** What is the term commonly used for the cloud's capability to scale outward and inward automatically based on demand?
- a.** Agility
 - b.** Reliability
 - c.** Elasticity
 - d.** Fault tolerance
- 3.** What is the very popular “as a Service” model that permits a cloud provider to make applications available that are typically accessible from anywhere?
- a.** IaaS
 - b.** SaaS
 - c.** PaaS
 - d.** GaaS
- 4.** What is the main “virtual machine” creation technology available in AWS?
- a.** S3
 - b.** EC2
 - c.** Route 53
 - d.** ELB

5. What is the object-based storage solution in AWS?

- a. S3
- b. EC2
- c. VPC
- d. IAM

6. Where are your own private subnets located in AWS?

- a. IAM
- b. EC2
- c. Lambda
- d. VPC

FOUNDATION TOPICS

INTRODUCTION TO THE CLOUD

To help us define the “cloud,” we turn to the National Institute for Standards and Technology (NIST). You can find this beneficial site at <https://www.nist.gov/>. According to the NIST, cloud computing is “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”



This statement certainly says a lot, and we really need to break it down. Fortunately, the NIST helps us with this as well. Here are the essential cloud characteristics you should be aware of:

- **On-demand self-service:** This characteristic means that a customer of cloud technologies (even if you are a customer of your own company's private cloud) can provision and manage resources without the intervention of cloud-hosting administrative personnel. For example, you might deem that you need a new web server to advertise a particular product or service. You can completely provision, configure, and deploy this web server without contacting anyone responsible for hosting the cloud solution.
- **Broad network access:** This aspect of cloud states that your cloud resources should be available over the network and accessed through standard mechanisms. These standard access approaches (such as HTTPS) promote the use of cloud by thin or thick client platforms (for example, mobile phones, tablets, laptops, and workstations).
- **Resource pooling:** The provider's computing resources are pooled to serve multiple clients using a multitenant model. This model allows multiple customers to securely use the same physical hardware of the provider. At any time, the cloud provider can use different physical and virtual resources dynamically assigned and reassigned according to consumer demand. You should note that this approach provides a sense of location independence in that the customer generally has no control or knowledge over

the exact location of the provided resources. If required, the customer is typically able to specify location at a higher level of abstraction (such as country, state, or geographical zone). Examples of resources that are typically pooled include storage, processing, memory, and network bandwidth.

- **Rapid elasticity:** Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward in accordance with demand from customers. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- **Measured service:** Cloud systems automatically control and optimize resource use by leveraging a metering capability. This is done by the provider at some level of abstraction appropriate to the type of service. For example, the metering might be based on storage, processing, bandwidth, or active user accounts. Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. This is where the cloud services your IT department pays for are often compared to a utility bill. Like with the electric bill, you can be billed monthly, for just those services you used.



Another excellent way to make sense of the many cloud technologies today is to break them down by the “as a

Service” category they fall under. The concept of “as a Service” means that customers “subscribe” to IT resources as needed. The “as a Service” technologies we see today include the following:

- **Software as a Service (SaaS):** This is currently the most popular cloud model. Here the customers access a provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser, or a program’s interface. Note that in this model, the customer does not manage or control the underlying cloud infrastructure, with the possible exception of limited user-specific application configuration settings.
- **Platform as a Service (PaaS):** This model provides a cloud infrastructure to the customer. This permits the customer to deploy onto the cloud infrastructure consumer-created or acquired applications developed for the cloud. The provider ensures the required programming languages, libraries, services, and tools are available for the customer. Typically, this is done on a pay-per-use or charge-per-use basis. Note that in this case, a cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources necessary to support the cloud services being provided, and typically includes server, storage, and network components. The abstraction layer

consists of the software deployed across the physical layer, which manifests the essential cloud characteristics.

Conceptually the abstraction layer sits above the physical layer. Notice also that the customer does not manage or control the underlying cloud infrastructure, including the network, servers, operating systems, and storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

- **Infrastructure as a Service (IaaS):** Allows the customer to provision processing, storage, networks, and other fundamental computing resources. The customer is then able to deploy and run arbitrary software, which can include operating systems and applications. The customer does not manage or control the underlying cloud infrastructure, but has control over operating systems, storage, and deployed applications. The customer might also have limited control of select networking components such as host firewalls.



How are cloud technologies commonly deployed? These deployment models are all in practice today:

- **Private cloud:** The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers, which of course might be business units. It might be owned, managed, and operated by the

organization, a third party, or some combination of both, and it might exist on or off premises.

- **Community cloud:** The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (for example, an overall mission or shared security requirements). It might be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of both. It might exist on or off premises.
- **Public cloud:** The cloud infrastructure is provisioned for open use by the general public. It might be owned, managed, and operated by a business, academic institution, or government organization, or some combination of the three. It exists on the premises of the cloud provider.
- **Hybrid cloud:** The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability. This is a widespread deployment model today.

INTRODUCTION TO THE AWS CLOUD

It is time to examine (at a high level) just some of the service categories in the AWS Cloud and the services and tools in each. This section provides this vital introduction for you.



Compute Service

AWS offers many different options for your acquisition and execution of computing resources. This section provides an overview of these many services:

- **Elastic Compute Cloud (EC2):** EC2 is a web service that provides secure and resizable compute resources in the AWS Cloud. The EC2 service allows you to provision and configure capacity with minimal effort. It provides you with easy control of your computing resources. EC2 reduces the time required to obtain and boot new servers (EC2 instances) to minutes. This efficiency allows you to scale capacity vertically (up and down, making your server resources bigger or smaller, respectively) and horizontally (out and in, adding more capacity in the form of more instances) as your computing requirements change. We call this remarkable quality “elasticity,” and we cover that in greater detail in Chapter 2, “Advantages of the AWS Cloud.” Figure 1-1 shows two virtual machines running in AWS EC2.

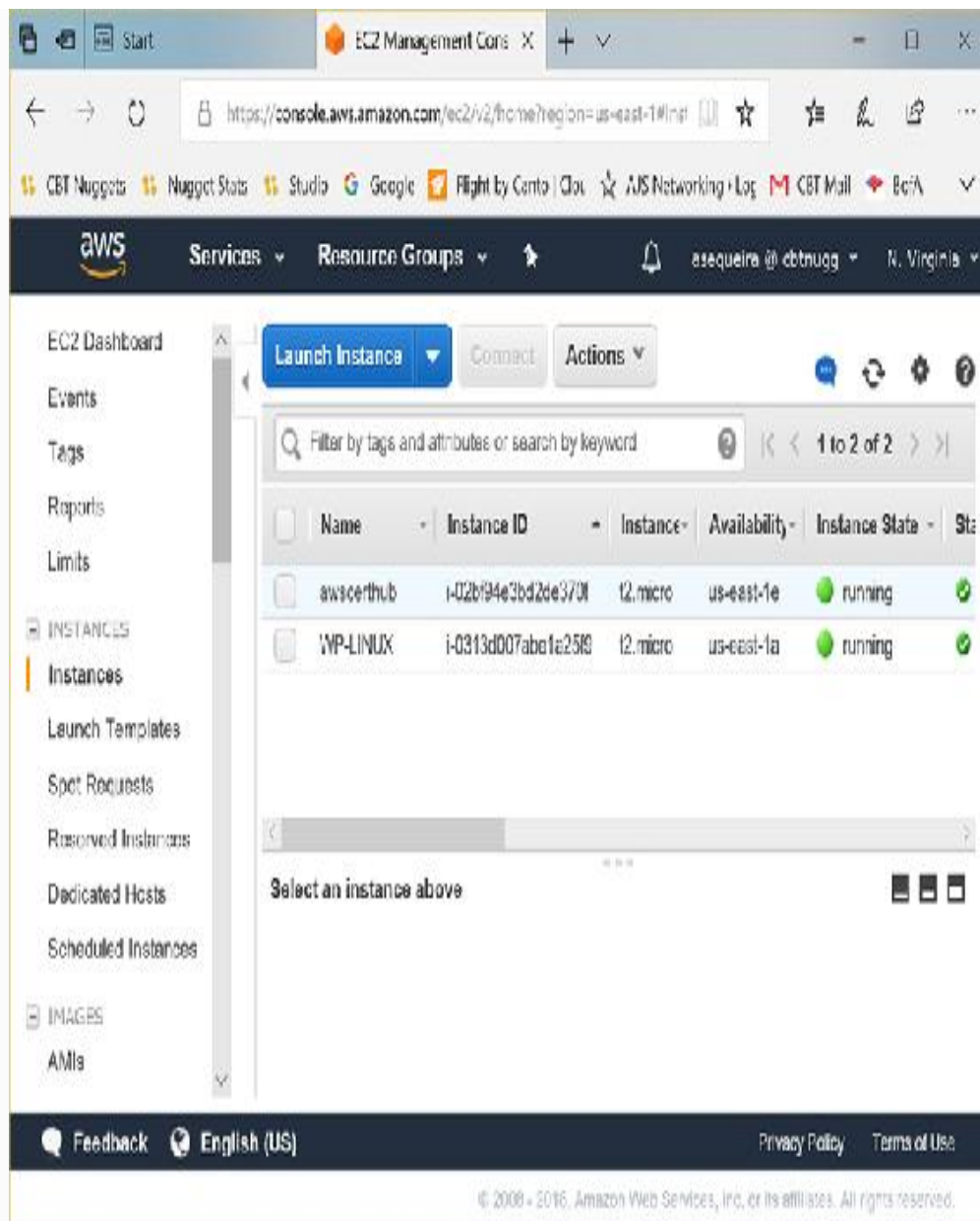


Figure 1-1 EC2 in AWS

- **Lambda:** AWS Lambda lets you run code without the burden of provisioning or managing servers. This code you run against Lambda can be for various aspects of an application or service. When you use Lambda, you upload your code, and Lambda does everything required to run

and scale your code with high availability and fault tolerance. Again, you are not required to provision or configure any server infrastructure yourself. Figure 1-2 shows the Lambda graphical user interface (GUI) in AWS.

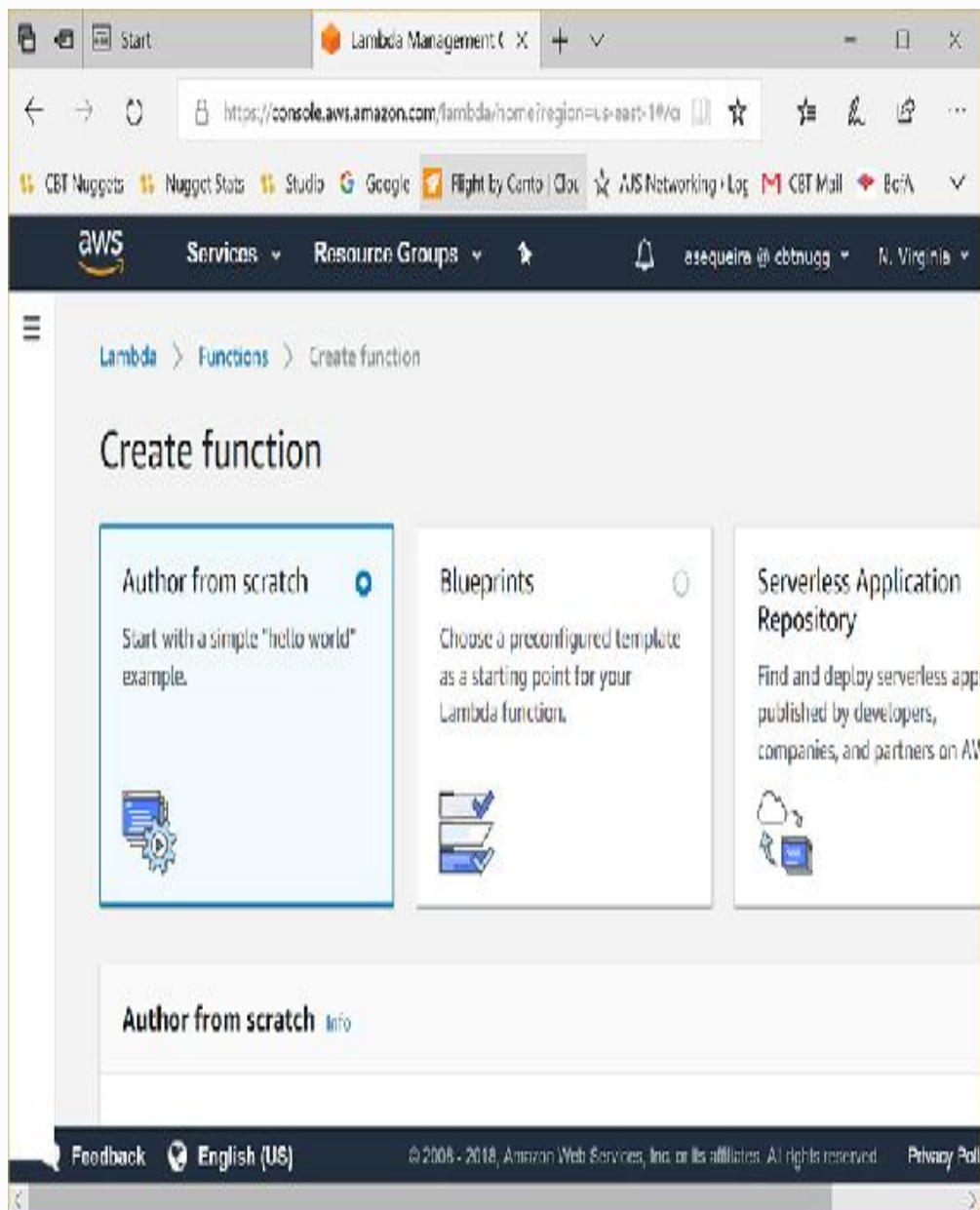


Figure 1-2 AWS Lambda

- **Elastic Beanstalk**: AWS Elastic Beanstalk is an easy-to-use service for deploying and scaling web applications and services developed with popular languages such as Java, PHP, and Python, to name a few. These web applications are run on familiar servers such as Apache, Nginx, Passenger, and Internet Information Services (IIS). Amazingly, with this service, you upload your code, and Elastic Beanstalk automatically handles the deployment, from capacity provisioning to load balancing, auto-scaling, and application health monitoring. Figure 1-3 shows the GUI interface of Elastic Beanstalk.

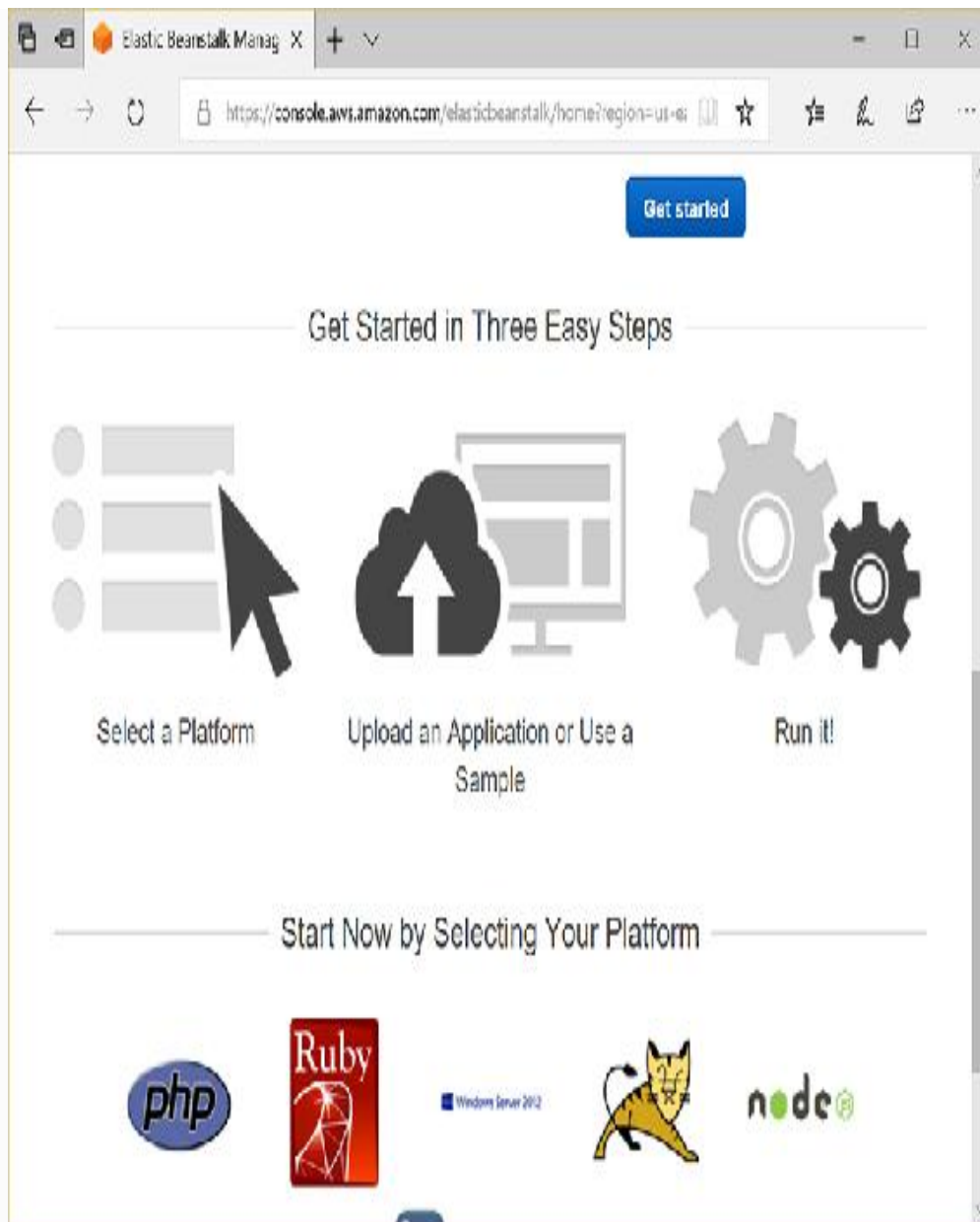


Figure 1-3 Elastic Beanstalk in AWS

- **Elastic Container Service (ECS):** The Amazon Elastic Container Service is a highly scalable, high-performance container management service that supports Docker containers. ECS permits you to run applications on a managed cluster of EC2 instances efficiently. It eliminates

the need for you to install, operate, and scale your own cluster management infrastructure.

Storage Services

The demands placed on storage for digital information today is higher than ever—and getting bigger all the time. It is no wonder that AWS offers many services in this regard. The list that follows highlights the important ones we will discuss further in this text:

- **Simple Storage Service (S3):** The AWS Simple Storage Service is object storage with a simple web service interface to store and retrieve any amount of data from anywhere on the web. It is designed to deliver 99.999999999% durability. You can use Amazon S3 for a vast number of purposes, such as primary storage for cloud-native applications or a bulk repository (or “data lake”) for analytics. It is so flexible and so easy to work with, there are far too many potential uses to list!
- **Elastic Block Store (EBS):** Elastic Block Store provides persistent block storage volumes for use with EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability. EBS volumes offer the consistent and low-latency performance needed to run your workloads. With Amazon EBS, you can scale your usage up or down within minutes—all while paying a low price for only what you provision.

- **Glacier:** Amazon Glacier is a secure, durable, and extremely low-cost storage service for data archiving and long-term backup. With Glacier you can reliably store large or small amounts of data for as little as \$0.004 per gigabyte per month. Glacier provides three options for access to archives, from a few minutes to several hours.
- **Elastic File System (EFS):** Amazon Elastic File System provides simple, scalable file storage for use with Amazon EC2 instances in the AWS Cloud, or can even be used by on-premises servers in your organization. EFS is easy to use and offers a simple interface that allows you to create and configure file systems quickly and easily.

Network Services

Where would we be without the network? Well, back to the Sneakernet, I suppose. Here are some of the critical networking services we discuss in this text:

- **Virtual Private Cloud (VPC):** Amazon Virtual Private Cloud lets you provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including a selection of your IP address range, the creation of subnets, and configuration of route tables and network gateways. You can use both IPv4 and IPv6 in your VPC for secure and easy access to resources and applications. [Figure 1-4](#) shows elements inside the VPC.

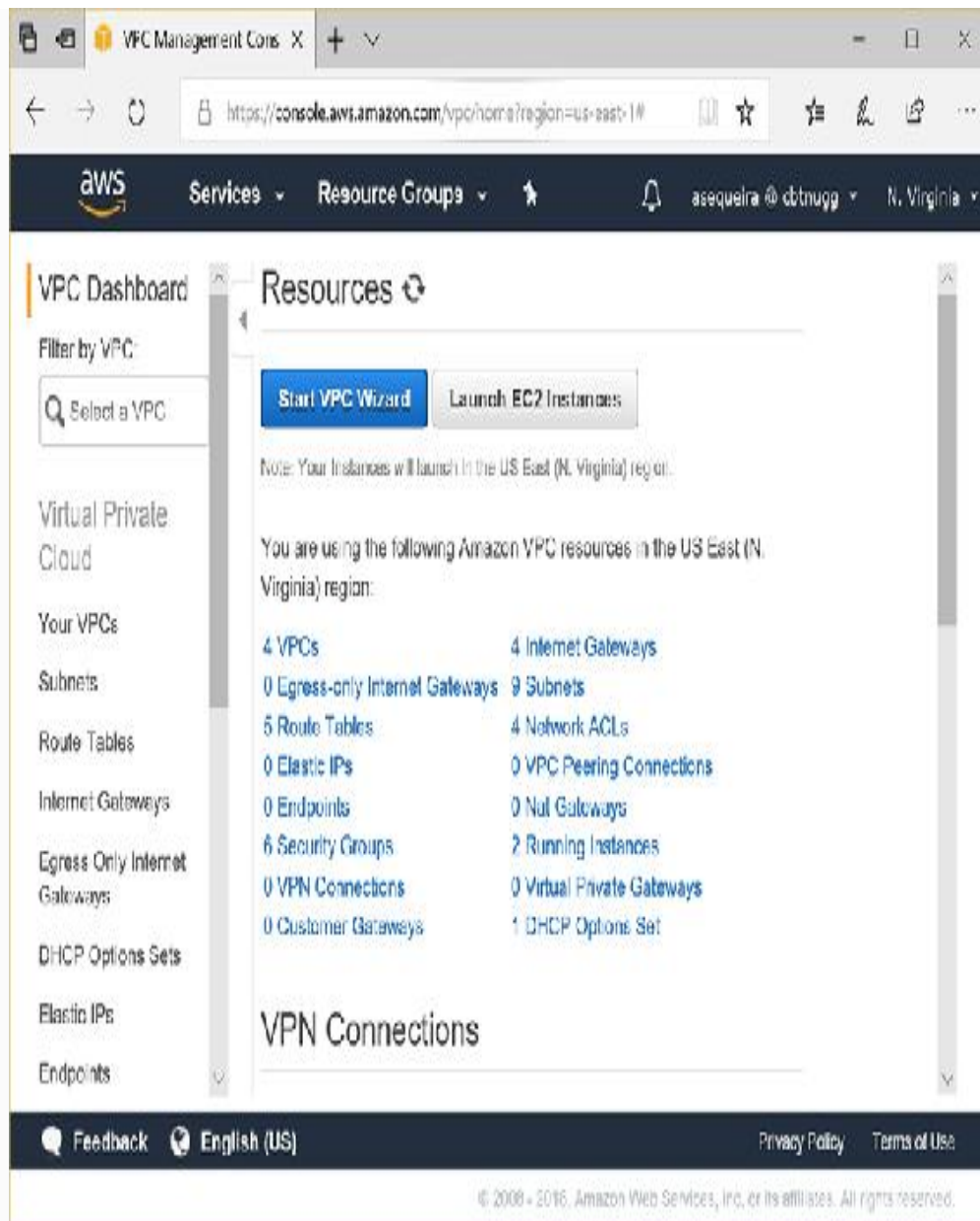


Figure 1-4 The Components of the AWS VPC

- **Route 53:** Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service. Route 53 effectively directs user requests to infrastructure running in AWS—such as EC2 instances, Elastic Load Balancing load balancers, or S3 buckets—and can also be

used to route users to infrastructure outside of AWS. You can use Route 53 to configure DNS health checks to route traffic to healthy endpoints or to monitor the health of your application and its endpoints independently.

- **CloudFront:** Amazon CloudFront is a global content delivery network (CDN) service. This service accelerates delivery of your websites, APIs, video content, or other web assets. The service automatically routes requests for your content to the nearest edge location, so it delivers content with the best possible performance.
- **API Gateway:** Amazon API Gateway is a fully managed service that makes it easy for developers to create, publish, maintain, monitor, and secure APIs at any scale. With a few clicks in the AWS Management Console, you can create an API that acts as a “front door” for applications to access data, business logic, or functionality from your back-end services, such as workloads running on EC2, code running on AWS Lambda, or any web application.
- **Direct Connect:** AWS Direct Connect is a solution that makes it easy to establish a dedicated network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your private network. In many cases can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

Database Services

There are many different approaches to databases these days, as our data needs have grown more varied and complex. Fortunately, AWS does a great job of keeping up with the advancements in a variety of services:

- **Relational Database Service (RDS)**: Relational Database Service makes it easy to set up, operate, and scale a relational database in the cloud. RDS provides six database engines to choose from: Aurora, PostgreSQL, MySQL, MariaDB, Oracle, and Microsoft SQL Server.
- **DynamoDB**: Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale. It is a great fit for mobile, web, gaming, ad tech, Internet of Things (IoT), and many other applications.
- **ElastiCache**: ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory caches, instead of relying entirely on slower disk-based databases. Interestingly, ElastiCache is not an AWS proprietary solution and runs the standardized Redis or Memcached solutions.
- **Redshift**: Redshift is a fast, fully managed, petabyte-scale data warehouse that makes it simple and cost-effective to analyze all your data using your existing business intelligence tools.

Security Services

It is incredible to think that if you do it correctly, you can be more secure with the cloud than with any approach you could take by yourself in your own data center. Here are the major technologies in the security area you should be aware of:

- **Identity and Access Management (IAM):** AWS Identity and Access Management (IAM) enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. [Figure 1-5](#) shows IAM in the GUI of AWS.

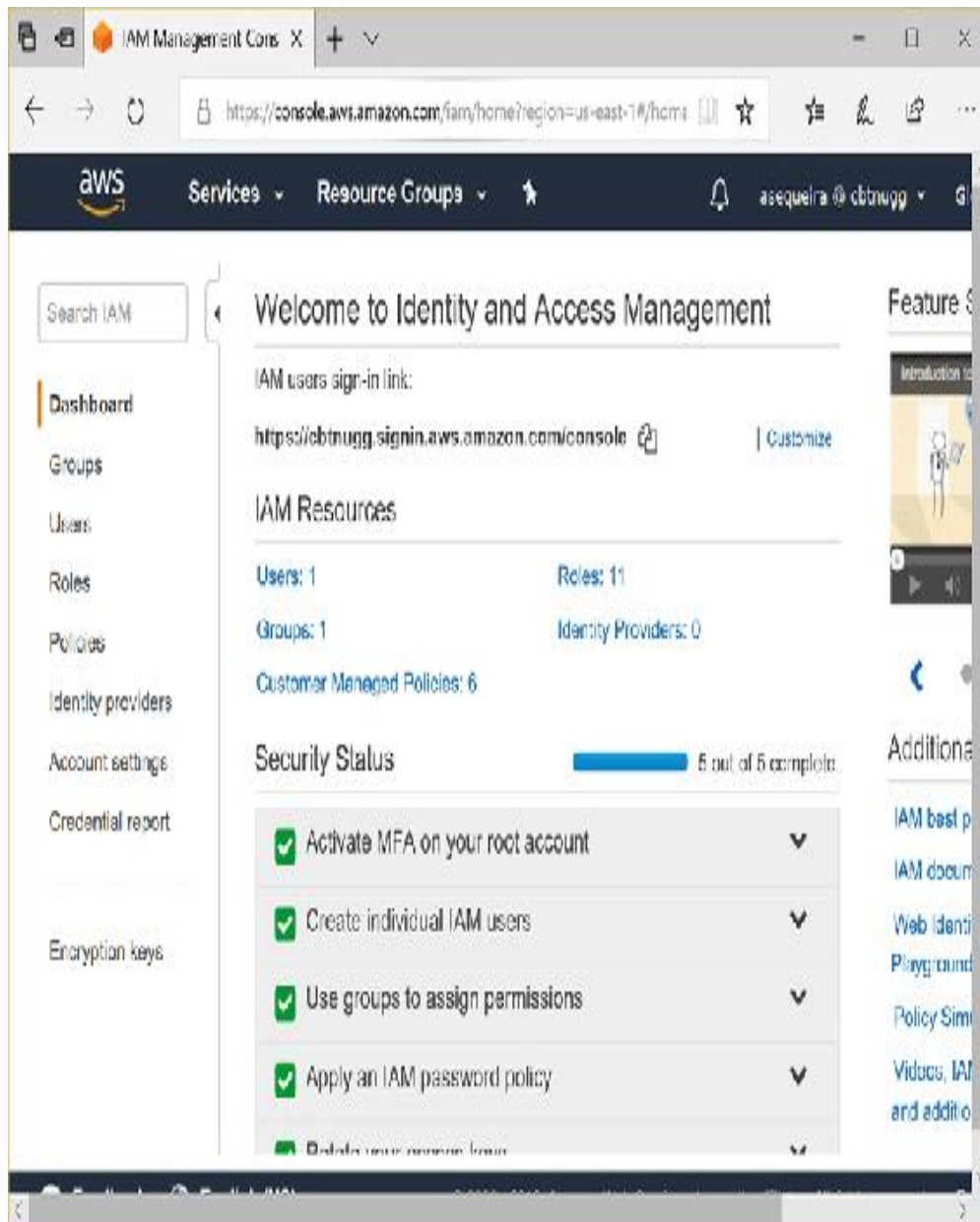


Figure 1-5 IAM in AWS

- **Security groups:** AWS security groups are associated with EC2 instances and provide security at the protocol and port access level. Each security group contains a set of rules that filter traffic coming into and out of an EC2 instance. If there is no rule that explicitly permits a particular data

packet, it will be dropped. Security groups also can be applied to many other services within your VPC, including ELB, RDS, Redshift, ElastiCache, and others.

- **Network ACLs**: Network access control lists are used to control traffic moving between your AWS VPC subnets. They function like traditional access control lists and are made up of permit and deny entries for various address and ports.

Automation and Application Support

There are many tools that foster the deployment of applications and automation in AWS. Here are some of the major ones:

- **CodeDeploy**: AWS CodeDeploy is a fully managed deployment service that automates software deployments to a variety of compute services such as EC2, Lambda, and your on-premises servers. CodeDeploy makes it easier for you to rapidly release new features, helps you avoid downtime during application deployment, and handles the complexity of updating your applications.
- **CloudFormation**: AWS CloudFormation gives you an easy way to provision and configure related AWS resources based on a template. The tool even offers a designer that permits you to build architectures in templated code from your “sketches” using the design tool.
- **OpsWorks**: AWS OpsWorks is a configuration management service that uses Chef or Puppet. These are

automation platforms that treat server configurations as code. OpsWorks uses Chef or Puppet to automate how servers are configured, deployed, and managed across your EC2 instances or on-premises compute environments.

Management Tools

Here are just some of the tools available to help you manage all that important stuff in the AWS cloud.

- **Service Catalog**: AWS Service Catalog allows organizations to create and manage catalogs of IT services that are approved for use on AWS. These IT services can include everything from virtual machine images, servers, software, and databases to complete multitier application architectures. AWS Service Catalog allows you to centrally manage commonly deployed IT services. It helps you achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved IT services they need.
- **Systems Manager**: AWS Systems Manager gives you visibility and control of your infrastructure on AWS. Systems Manager provides a unified user interface so you can view operational data from multiple AWS services and allows you to automate operational tasks across your AWS resources. With Systems Manager, you can group resources (EC2 instances, S3 buckets, or RDS instances) by application, view operational data for monitoring and troubleshooting, and take action on your groups of resources.

- **Trusted Advisor**: AWS Trusted Advisor is an online resource to help you reduce cost, increase performance, and improve security by optimizing your AWS environment. Trusted Advisor provides real-time guidance to help you provision your resources following AWS best practices.

Monitoring

Do you need to track accurately the performance and status of your resources and services? There are tools for that too in AWS.

- **CloudWatch**: Amazon CloudWatch is a monitoring service for AWS Cloud resources and the applications you run on AWS. CloudWatch can collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.
- **CloudTrail**: AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. Features include detailed reports of recorded information, which can include the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service.

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the

exercises here, Chapter 16, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 1-2 lists these key topics and the page numbers on which each is found.



Table 1-2 Key Topics for Chapter 1

Key Topic Element	Description	Page Number
List	Cloud characteristics	
List	As a Service models	
List	Deployment models	
List	Compute services	

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

Elasticity

SaaS

PaaS

IaaS

private cloud

community cloud

public cloud

hybrid cloud

EC2

Lambda

Elastic Beanstalk

ECS

S3

EBS

Glacier

EFS

VPC

Route 53

CloudFront

API Gateway

Direct Connect

RDS

DynamoDB

ElastiCache

Redshift

IAM

security groups

network ACLs

CodeDeploy

CloudFormation

OpsWorks

Service Catalog

Systems Manager

Trusted Advisor

CloudWatch

CloudTrail

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. Name at least three cloud characteristics as defined by NIST.
2. Name the three major “as a Service” models of cloud.
3. Name the four cloud deployment models.
4. What was the first serverless compute service of AWS?
5. What AWS feature permits you to create persistent storage volumes for use by EC2 instances (including boot)?
6. What monitoring tool permits you to carefully observe specific API calls to AWS resources?

Chapter 2

Advantages of the AWS Cloud

This chapter covers the following subjects:

- **Cloud Advantages:** This section covers just some of the many advantages of cloud technologies in general. This section is not specific to Amazon Web Services (AWS), but AWS does provide all the benefits covered. The AWS-specific advantages are elaborated on in the section that follows.
- **AWS Cloud Advantages:** This part of the chapter focuses on the specific advantages AWS brings and references many of the specific technologies that make them a reality.

Why are cloud engineers in such high demand? In fact, why is the cloud so popular today to begin with? This chapter ensures you understand the many advantages we realize with cloud technology adoption, and then the chapter gets very specific to AWS. This chapter examines AWS-specific benefits and some of the many technologies that make them a reality.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. [Table 2-1](#) lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 2-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions
Cloud Advantages	1–3
AWS Cloud Advantages	4–6

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. What replaces CapEx as an advantage of the cloud?
 - a. FIFO
 - b. GARP
 - c. ROI
 - d. OpEx

2. What model is often followed in order to charge for cloud usage?
- a.** Pay as you terminate
 - b.** Pay as you go
 - c.** Pay as you can
 - d.** Pay as you will
3. What is the large advantage to the cloud's emphasis on APIs?
- a.** Cost
 - b.** Automation
 - c.** Simple learning curve
 - d.** Lack of traceability
4. Which of the following is not a major contributor to the agility that AWS provides?
- a.** Governance
 - b.** Speed
 - c.** The culture of innovation
 - d.** Experimentation
5. What major global architecture component exists in regions?
- a.** Offline stores
 - b.** Availability Zones
 - c.** Hotspots

- d. Clusters
6. Which of the following is not a form of ELB in AWS?
- a. Application Load Balancer
 - b. Classic Load Balancer
 - c. Network Load Balancer
 - d. Virtual Load Balancer

FOUNDATION TOPICS

CLOUD ADVANTAGES



It is no major surprise that various public cloud vendors (led by AWS) are experiencing more success than ever before. The list of advantages continues to grow! Here are just some:

- **CapEx is replaced by OpEx:** Using public cloud technologies enables startups and existing organizations to provide new features and services with a minimum of capital expenditures (CapEx). Instead, public cloud expenses revolve around monthly operating expenses (OpEx). For most organizations, OpEx represents significant advantages when compared to significant CapEx investments.
- **Lack of contractual commitments:** Many public cloud vendors charge on an hourly (if not less) basis. For most

services, there is no long-term commitment to an organization. You can roll out new projects or initiatives and, if needed, roll back with no contractual commitments long term. This lack of contractual commitment helps increase the agility of IT operations and lowers financial risks associated with innovative technologies.

- **Reduction of required negotiations:** New account establishment with public cloud vendors is simple, and prices for the major public cloud vendors continuously reduce. This reduction in prices and the ease of account setup reduces the need for cost negotiations, as might have existed early in the world of service provider interactions.
- **Reduced procurement delays:** Additional resources can be set up with most cloud implementations within seconds.
- **“Pay as you go” model:** If more resources are needed to support a growing cloud presence, you can get these resources on demand and pay for them only when needed. Conversely, if fewer resources are required, you can run less and pay for only what you need. Figure 2-1 shows an example of a cost dashboard in AWS. Notice how each service is incurring a cost on a monthly basis and the costs are broken down, like a modern utility bill.

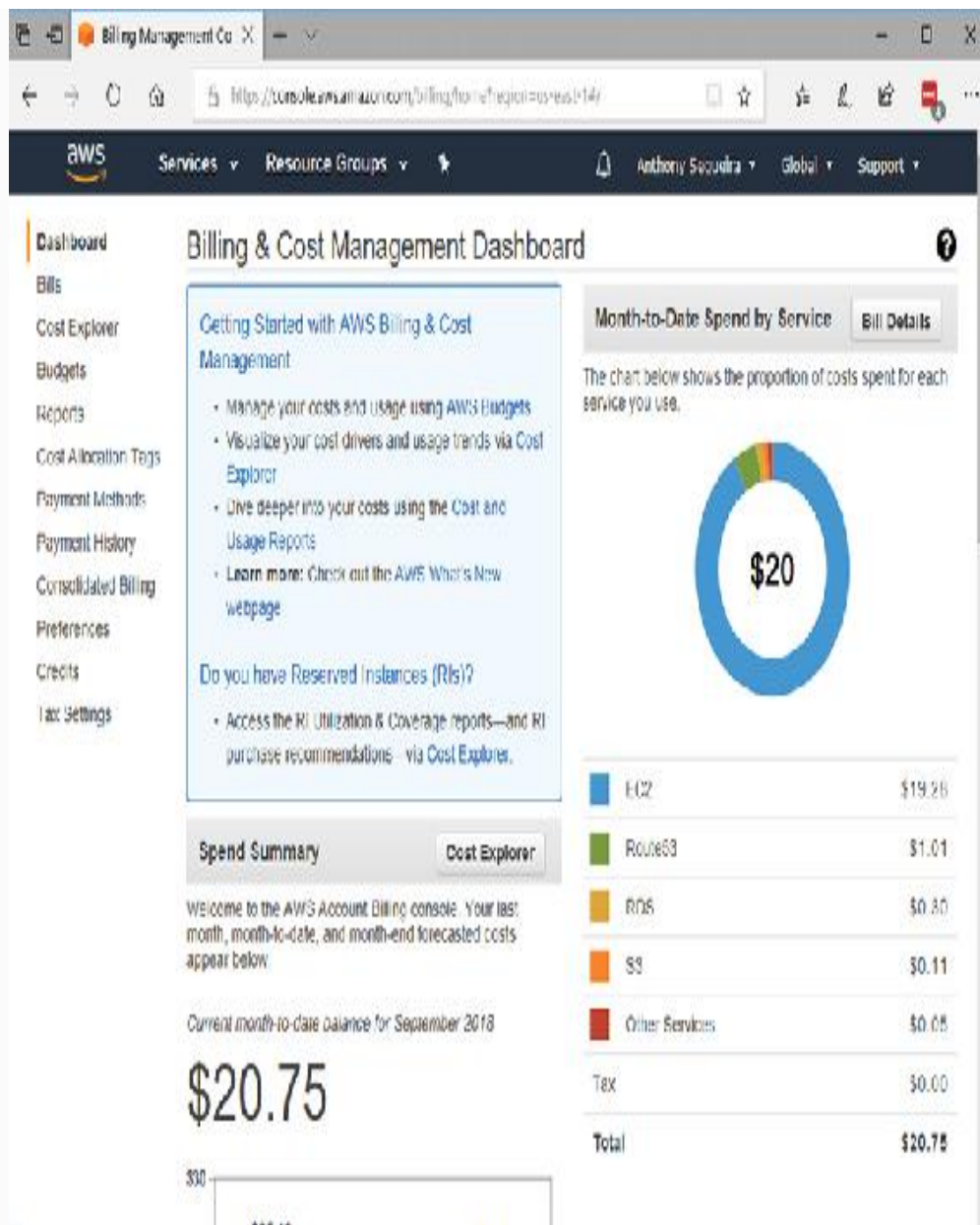


Figure 2-1 Costs in the Cloud Are “Pay as You Go”

- **High levels of security possible:** Because you can focus on the security of your resources and the cloud provider can focus on its security responsibilities (such as physical security and hypervisor security), the resulting infrastructure can meet stringent levels of security. This

security model is appropriately termed the *Shared Responsibility model*.

- **Flexibility:** Thanks to features in public cloud vendors like AWS, you can quickly scale the cloud-based infrastructure up and down as well as out and in, as needed. This advantage is often termed *elasticity*. Auto-scaling functionality inside of AWS allows the dynamic creation and destruction of resources based on actual client demand. Such scaling can occur with little to no administrator interaction. When discussing scaling the resources of a service, we are scaling those resources horizontally (out and in with elasticity), while the service made up of those resources is being scaled up and down (vertically because the single service is getting bigger or smaller). A single service scales up and down as well as out and in, depending on the context.
- **A massive global infrastructure:** Most of the public cloud vendors now offer resources located all over the globe. This global dispersion of resources serves large multinational organizations very well since resources needed for certain parts of the globe can be stored and optimized for access in those regions. Also, companies with clients all over the world can meet with similar access advantages when servicing the needs of clients.
- **SaaS, PaaS, and IaaS offerings:** Cloud technologies have become so advanced that organizations can choose to give applications to clients, development environments, or even entire IT infrastructures using the technologies that make

up the cloud. In fact, since cloud can offer about any component of IT these days, many refer to cloud as an *Everything as a Service (XaaS)* opportunity.

- **Emphasis on API support:** Increasingly, cloud vendors are taking an application programming interface (API) first approach. This makes the same configuration possible with REST APIs (typically used) that would be possible with an software development kit (SDK), command-line interface (CLI), or graphical user interface (GUI). The API first approach means no interface (CLI or GUI) changes are made until API calls are made first. Thus, there is nothing that cannot be automated! Figure 2-2 shows how the vast amount of AWS service can be accessed from a simple GUI called the AWS Management Console.

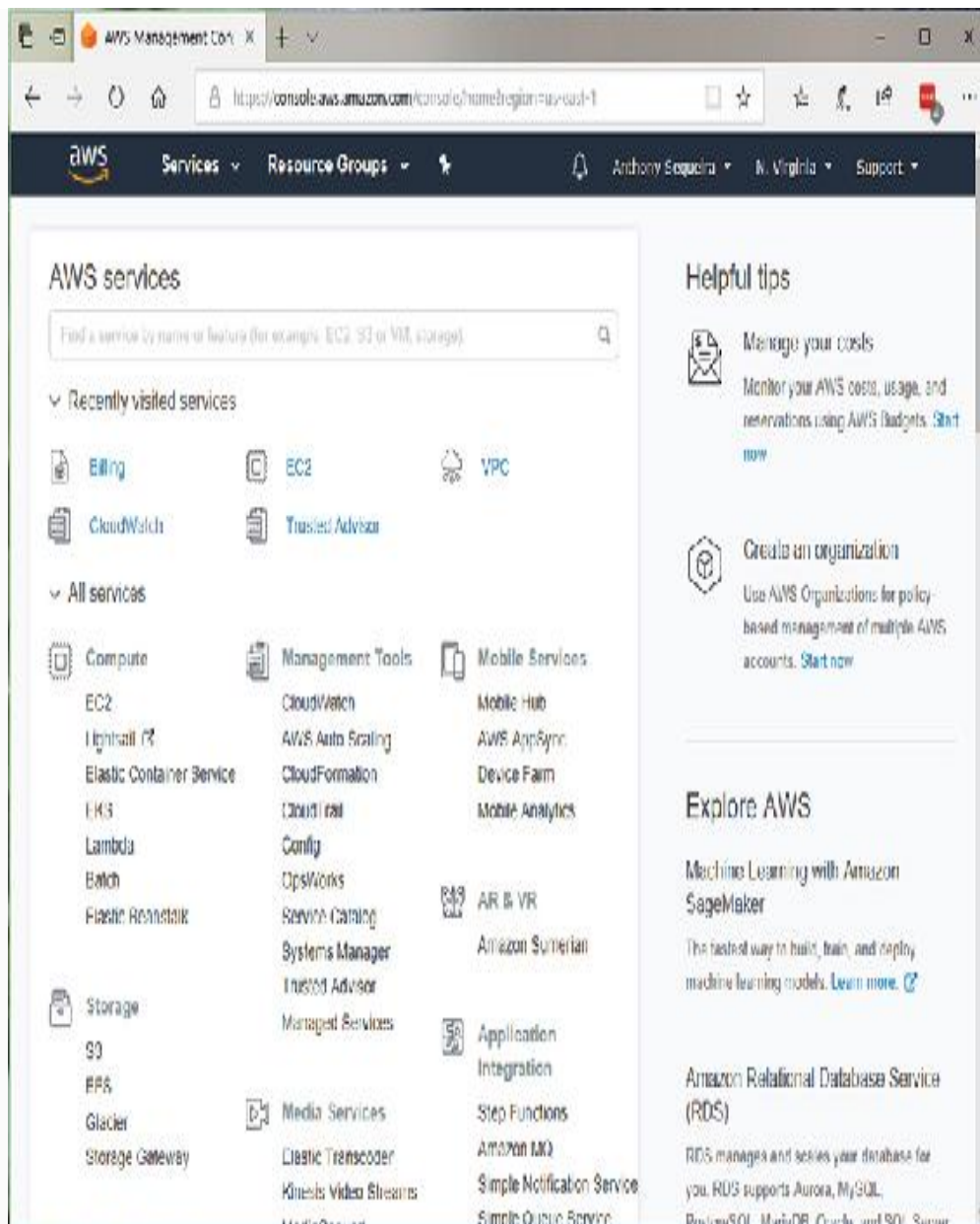


Figure 2-2 Managing Vast Cloud Resources in a Simple GUI

AWS CLOUD ADVANTAGES

The “pay as you go” model followed by AWS is a huge revolution in budgeting and affording the latest technological innovations. In fact, thanks to this simple model, engineers can

really focus on innovation and new business solutions instead of worrying about infrastructure and other resource shortfalls.

Before the broad adoption of AWS solutions, engineers would waste time and money over-provisioning resources in order to attempt to provide reliability and performance, even under peak load conditions. AWS allows cloud engineers to “spin up” new resources in seconds and view these resources as temporary and disposable. In fact, it is not uncommon for AWS customers to deploy massive amounts of infrastructure for a very short period of time in order to test new technologies without paying massive upfront costs. One great story I learned at an AWS re:Invent conference in 2017 was about a large university needing to conduct some artificial intelligence testing. The university turned to AWS for help and spun up millions of CPUs across hundreds of thousands of Elastic Cloud Compute (EC2) virtual machines (VMs). Sure enough, they only required this horsepower over the course of a weekend. All of the resources were “terminated” (that’s the AWS term for deleting an EC2 VM) once the testing was complete. Amazon did not tell us what the bill was for this weekend of work, but you can rest assured that the cost of all of those resources if purchased as a capital expense would have been massive. And what would the company do with the resources once the testing was complete?

Amazon Web Services truly enables an organization to be flexible with the provisioning of resources because there are much fewer constraints. Efficiency is also achieved since the duration to provision new resources is remarkably small.



One of the most significant advantages companies see in moving to AWS is the ability to increase their agility. There are three main aspects of AWS that accomplish this:

- **Speed:** The AWS Global Infrastructure spans the entire globe. This global reach ensures you can place resources geographically close to those that need to consume them. This reduces latency and fosters excellent performance. As described earlier, massive amounts of resources can be provisioned within seconds in the AWS cloud.
- **Experimentation:** With AWS, you can take your IT operations and implement them as code. In addition to running with administrative ease and error-free, this fosters the ease of experimentation and testing. Templates are available thanks to services like AWS CloudFormation that permit you to instantly create complex networks and IT resources for testing and experimenting with. Remember, once the experimentation is done, you can dispose of the resources and are no longer charged for their use. Figure 2-3 shows an example of CloudFormation.

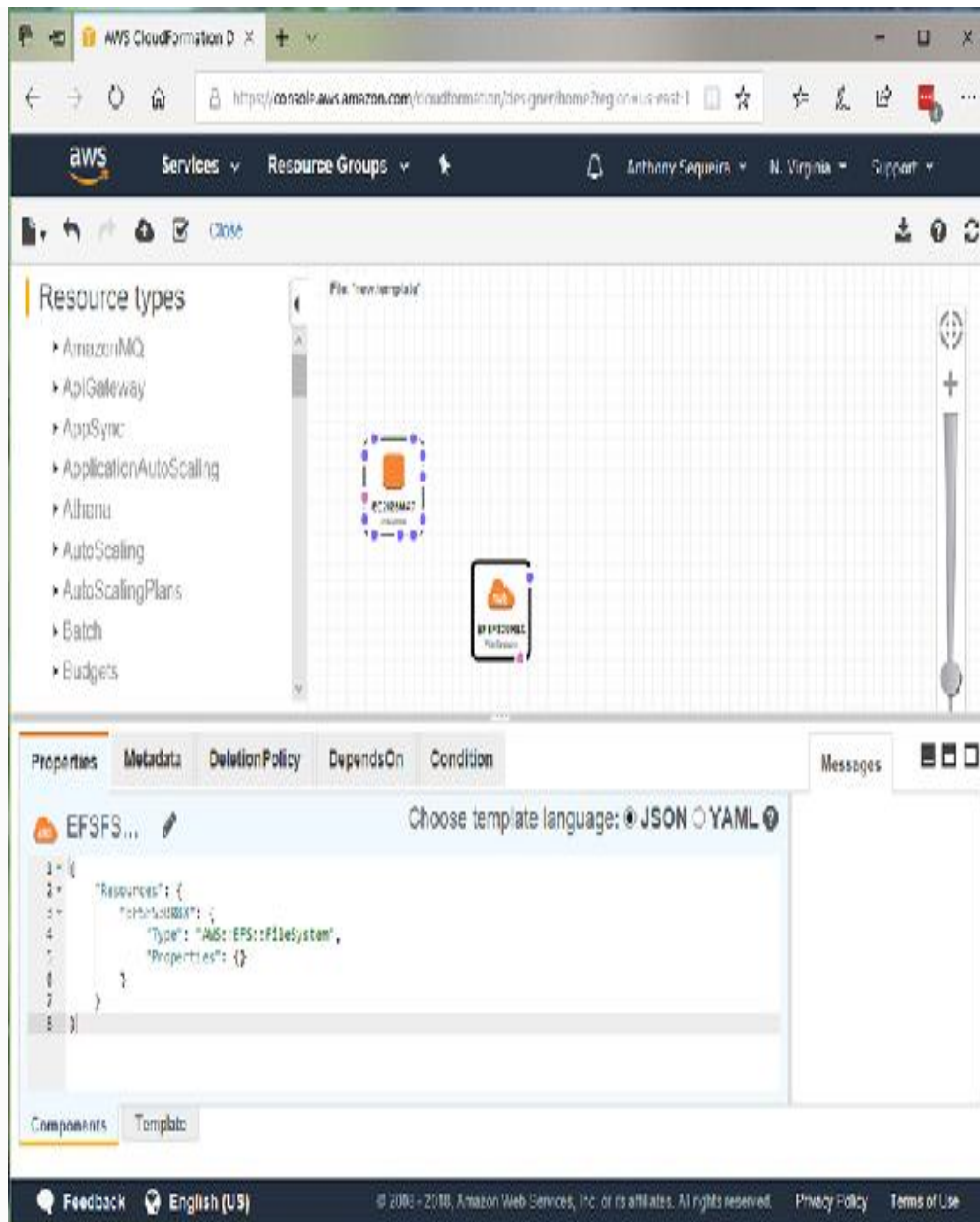


Figure 2-3 CloudFormation in AWS

- **Culture of innovation:** These enablers of agility previously listed also help foster a culture of innovation in your enterprise. In fact, an increasing number of companies participate in AWS functions because of this. It is no longer merely about saving costs for them. They love

the ability to experiment with new technologies at a very low risk to their organization. New innovations are thought of as very possible thanks to AWS.



Perhaps at the very core of AWS is what makes it all possible—the AWS Global Infrastructure. This is what makes the incredible elasticity, scalability, and reliability possible across a vast number of IT services. The AWS Global Infrastructure is made up of many components, but here are the two you should master now:

- **Regions**: Regions are physical locations in geographically dispersed parts of the globe. For example, there are US West regions and US East regions, just as there are regions in Europe and Asia. Inside of each region are multiple Availability Zones (AZs). These AZs house the data centers that actually contain the physical network resources and the massive amounts of data.
- **Availability Zones**: AZs are made up of one or more data centers. These data centers are filled with redundancy at every level, from network connections, to physical devices. The data centers are also physically distant from one another in order to help mitigate the effects of localized disasters. They feature incredible high availability (HA) and fault tolerance (FT).

Figure 2-4 demonstrates how easy it is to drop a menu at the top of the management console in order to select a new region

of the world for the initialization of localized resources for that region.

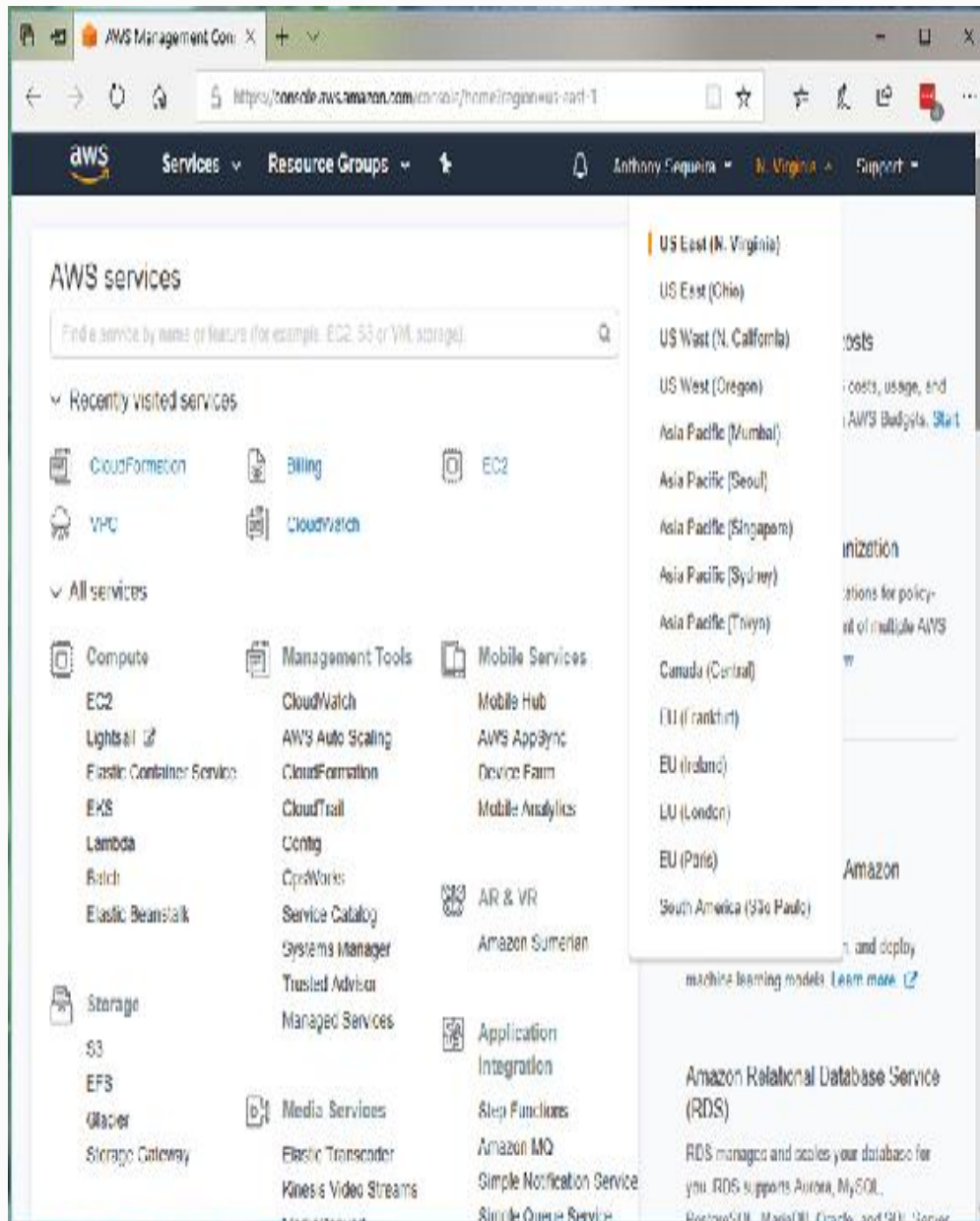


Figure 2-4 Selecting a Region in AWS

Another huge advantage that AWS brings is the use of easy-to-use tools that foster overall cloud benefits such as elasticity.

There are two tools in particular you should be aware of:

- **Auto Scaling**: Auto Scaling monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost. Thanks to this powerful tool, you can enable application scaling for multiple resources across multiple services in minutes. The service provides a simple, powerful user interface that lets you build scaling plans for resources like Amazon EC2 instances.
- **Elastic Load Balancing**: Elastic Load Balancing (ELB) automatically distributes incoming application traffic across multiple targets, such as Amazon EC2 instances, containers, and IP addresses. It can handle the varying load of your application traffic in a single Availability Zone or across multiple Availability Zones. Elastic Load Balancing offers three types of load balancers that all feature the high availability, automatic scaling, and robust security necessary to make your applications fault tolerant. These three types are the Application Load Balancer, the Network Load Balancer, and the Classic Load Balancer. Figure 2-5 shows the configuration of the Network Load Balancer in AWS.

The screenshot displays the AWS Management Console interface for configuring an Elastic Load Balancing (ELB) instance. The browser window title is 'EC2 Management Console'. The URL bar shows 'https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#V2>CreateELB'. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information 'asequeira @ dbmugg' in 'N. Virginia' with a 'Support' link.

The main content area is titled 'Step 1: Configure Load Balancer' and includes a progress bar with four steps: '1. Configure Load Balancer' (active), '2. Configure Routing', '3. Register Targets', and '4. Review'.

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives TCP traffic on port 80.

Name (i)

Scheme (i) ☒ Internet-facing ☐ Internal

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port
<input type="text" value="TCP"/>	<input type="text" value="80"/>

At the bottom of the console, there is a footer with 'Feedback', 'English (US)', '© 2006 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

Figure 2-5 Elastic Load Balancing in AWS

Another huge advantage that AWS brings is in the area of security and compliance. Thanks to the AWS Global Infrastructure, you maintain control of where your resources are stored geographically, and this makes it easier for you to comply with regional governance responsibilities. AWS

permits you to achieve the strictest security requirements, and you rest at ease knowing that AWS uses the most cutting-edge security-heavy data centers in the world.

You also enjoy vast amounts of reliability for your AWS projects. This helps you deliver high performance, permits ease with failure recovery, and permits you to acquire new resources, as needed, dynamically and with high speed.

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the exercises here, [Chapter 16, “Final Preparation,”](#) and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. [Table 2-2](#) lists these key topics and the page numbers on which each is found.



Table 2-2 Key Topics for [Chapter 2](#)

Key Topic Element	Description	Page Number
List	Cloud advantages	
List	Factors fostering agility	
List	AWS Global Infrastructure major components	

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

CapEx

OpEx

API

agility

AWS Global Infrastructure

regions

Availability Zones

Auto Scaling

Elastic Load Balancing

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

- 1.** How is the region determined when you want to create virtual machines in AWS?
- 2.** What is actually being sent to your AWS resources when you make configuration changes in the GUI Management Console?
- 3.** Where are Availability Zones located in AWS?

Chapter 3

Core AWS Services

This chapter covers the following subjects:

- **Overview of Services and Categories:** In this section of the chapter, we lay out the most important categories of services you should be familiar with at this stage of your AWS education.
- **Introduction to the AWS Global Infrastructure:** This part of the chapter ensures you know the various components that make up all of the Amazon-owned data resources throughout the globe.
- **Introduction to Virtual Private Cloud:** The Virtual Private Cloud (VPC) is your own virtual networks inside the AWS Cloud. This part of the chapter ensures that you understand the possible components you can use.
- **Introduction to Security Groups:** Security groups are built-in (and often mandatory) firewalls you use to control traffic into and out of AWS resources. This part of the chapter describes them in detail for you.
- **Introduction to Compute Services:** The primary compute resource in AWS is the EC2 instance. This section of the chapter teaches you about EC2 and also

discusses an exciting alternative—serverless computing with Lambda in AWS.

- **Introduction to EBS:** This part of the chapter teaches you the basics of Elastic Block Store (EBS) storage in AWS. This storage is used frequently for the disks required by EC2 instances.
- **Introduction to S3:** This section of the chapter teaches you detailed information on the Simple Storage Service (S3) of AWS. This is flexible and reliability object-based storage that can serve many purposes for you.
- **Introduction to AWS Database Solutions:** It cannot be stressed enough how important database technology is, as it continues to drive IT. AWS provides many different options for cloud-based database solutions. This part of the chapter covers the most important ones as of the time of this writing.

It is important to realize that AWS is *always* adding services to their incredible existing lineup of IT cloud-based offerings. With that said, there are many services in AWS that we must consider as core. This is because they are mature, heavily used, and often raved about by Amazon customers. This chapter seeks to get you very familiar with these core services. This will not only help you when you go to implement your AWS solutions, but it will also help you on your exam, where you are expected to know these details very well.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. [Table 3-1](#) lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 3-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions
Overview of Services and Categories	1
Introduction to the AWS Global Infrastructure	2–3
Introduction to Virtual Private Cloud	4–5
Introduction to Security Groups	6–7
Introduction to Compute Services	8–10
Introduction to EBS	11
Introduction to S3	12–13
Introduction to AWS Database Services	14–15

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should

mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1.** What service category does CloudFront fall under?
 - a.** Compute Services
 - b.** Storage
 - c.** Networking and Content Delivery
 - d.** Security, Identity, and Compliance
- 2.** A region in AWS is broken up into what construct?
 - a.** Primary and secondary data centers
 - b.** Availability Zones
 - c.** Vaults
 - d.** Pods
- 3.** What Global Infrastructure component of AWS serves CloudFront content?
 - a.** Availability Zones
 - b.** Edge Locations
 - c.** Vaults
 - d.** Cache Centers
- 4.** What component can you use to connect your VPC to the public Internet?
 - a.** IGW

- b. IDS**
 - c. IPS**
 - d. NACLs**
- 5.** Where can you place your resources in a VPC to help ensure high availability?
- a. Different regions**
 - b. Different root accounts**
 - c. Different storage tiers**
 - d. Different AZs**
- 6.** What two protocols are commonly permitted in security groups in order to permit remote administration of systems? (Choose two.)
- a. RDP**
 - b. ICMP**
 - c. SFTP**
 - d. SSH**
- 7.** Security groups in AWS protect what resources?
- a. AZs**
 - b. Subnets**
 - c. EC2 instances (through ENIs)**
 - d. Vaults**
- 8.** What is a serverless compute service of AWS?
- a. Aurora**

- b.** Snowball
- c.** Glacier
- d.** Lambda

9. What is a PaaS service of AWS?

- a.** CloudFormation
- b.** CloudFront
- c.** Elastic Beanstalk
- d.** RDS

10. What EC2 pricing model allows you to bid on availability capacity?

- a.** Temporary instances
- b.** Spot instances
- c.** Reserved instances
- d.** On-demand instances

11. What is a common use of EBS in AWS?

- a.** To receive and process streaming data for IoT
- b.** To provide serverless compute resources
- c.** To act as the boot volume for an EC2 server instance
- d.** To makes files available to massive numbers of users and groups

12. How does S3 ensure the durability of your data?

- a.** Multiple high-speed Internet connections are made to every major directory you create.

- b.** Data is storage-tiered by default.
 - c.** Data is automatically replicated to an alternate region.
 - d.** Multiple copies of your data are stored in separate Availability Zones.
- 13.** What is the archiving/warehousing solution within S3?
- a.** Glacier
 - b.** Snowball
 - c.** EFS
 - d.** Aurora
- 14.** Which AWS database is a NoSQL database solution often being used with the IoT?
- a.** Aurora
 - b.** Glacier
 - c.** Snowball
 - d.** DynamoDB
- 15.** Which of the following is a data warehouse solution in AWS?
- a.** Redshift
 - b.** Aurora
 - c.** RDS
 - d.** ElastiCache

FOUNDATION TOPICS

OVERVIEW OF SERVICES AND CATEGORIES

There are many, many different services that make up AWS, with more being added all the time. As a result, there is also a growing list of AWS service categories. For example, years ago, machine learning would not have been a category within AWS, but now it is one garnering much attention, and soon it will have its own specialty certification in the AWS certification lineup. [Figure 3-1](#) shows just some of the service categories and services in AWS.

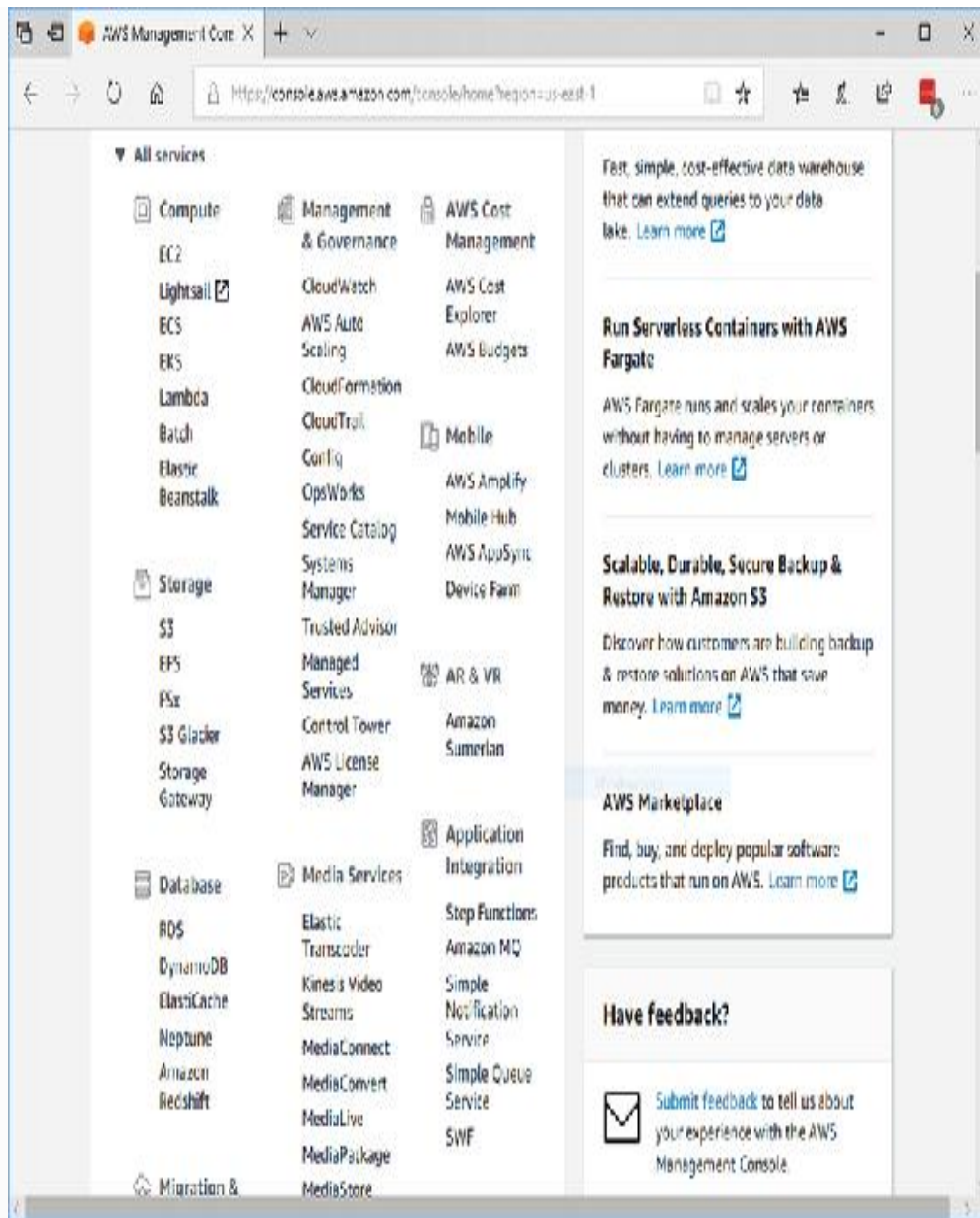


Figure 3-1 Some Service Categories in AWS

Note

Remember, you can always check out my AWS site (awscenterhub.com) for the latest versions of AWS certifications and their requirements.

Here are the main service categories you should be aware of at this point:

- Compute
- Storage
- Database
- Networking and Content Delivery
- Security, Identity, and Compliance

INTRODUCTION TO THE AWS GLOBAL INFRASTRUCTURE

The AWS Global Infrastructure is just that—it is global. It is made up of the latest and greatest networking and data center technologies, and it spans (almost) the entire globe.



To understand it, you should break the AWS Global Infrastructure down into three main components:

- **Regions**: Geographic locations that host two or more Availability Zones (AZs). You choose regions based on availability requirements for your resource locations, and you can even host resources in multiple regions to serve different customers in different locations. Regions are treated as separate entities and, by default, information does not transfer between regions. Finally, not all regions offer all AWS services.

- **Availability Zones (AZs)**: A collection of separate data centers in a region. The data centers are separated as much as possible for high availability, but they are connected together using very high-speed links. Each AZ in a region uses its own power provider (or multiple power providers) and has its own backup generators; some even have their own power substations.
- **Edge Locations**: These locations host cached content from your architecture for fast delivery to clients. The caching technology of AWS is called CloudFront. Edge Locations add even more low-latency reach to your clients (beyond the already amazing reach of regions and AZs). Edge Locations are also entry points into the AWS network, when using CloudFront or S3 Transfer Acceleration for data ingestion.

INTRODUCTION TO VIRTUAL PRIVATE CLOUD

When you think about virtual networking in the public cloud of AWS, think Virtual Private Clouds (VPCs). A VPC allows you to create private virtual networks and use the same concepts that you are already familiar with from traditional networking. With a VPC, you have complete control of your network configuration. You have the ability to isolate resources from or expose resources to the public Internet or to your private host systems inside your corporation.

With VPC, there are several layers of security controls (as you would expect). For example, you have security groups and

network access control lists (ACLs) that act as firewalls, to name just two. security groups control traffic in and out of your Elastic Compute Cloud (EC2) instances, whereas network ACLs permit the control of traffic in and out of your subnets in the VPC.

NOTE

While it is true that you use security groups to control traffic in and out of your EC2 instances, understand that they actually do this by controlling traffic in and out of the Elastic Network Interfaces (ENIs) used by your EC2 instances. So, for example, if you were to create a security group protecting one of your EC2 instances, and were to move its ENI to another EC2 instance, the security group protections would move as well.

When you are architecting solutions in AWS, you deploy various services and resources into your VPC in order to make up the full solution. You can even be very specific with service and resource placement so you know exactly where in your virtual network the resources reside. These services also conveniently inherit the security you have built into your network. Examples of services you would deploy into your VPC would be Elastic Compute Cloud, Elastic File System, Relational Database Services, Elastic Load Balancing, and many more.



Here are the main features of VPC you should be aware of:

- **High availability:** VPCs build upon the high availability built into AWS regions and Availability Zones (AZs). Your

VPCs live within a region, and you can have multiple VPCs per account.

- **Subnets:** Just like in your private network infrastructures, VPCs are made up of subnets that you can use to provide segmentation at Layer 3 (the Network layer).
- **Route tables:** You can use route tables to route traffic entering and exiting your subnets. You get this familiar model without needing to worry about the physical routers themselves.
- **Internet Gateway (IGW):** Permits easy-to-configure access to the Internet for your VPC; Figure 3-2 shows an Internet Gateway in AWS.

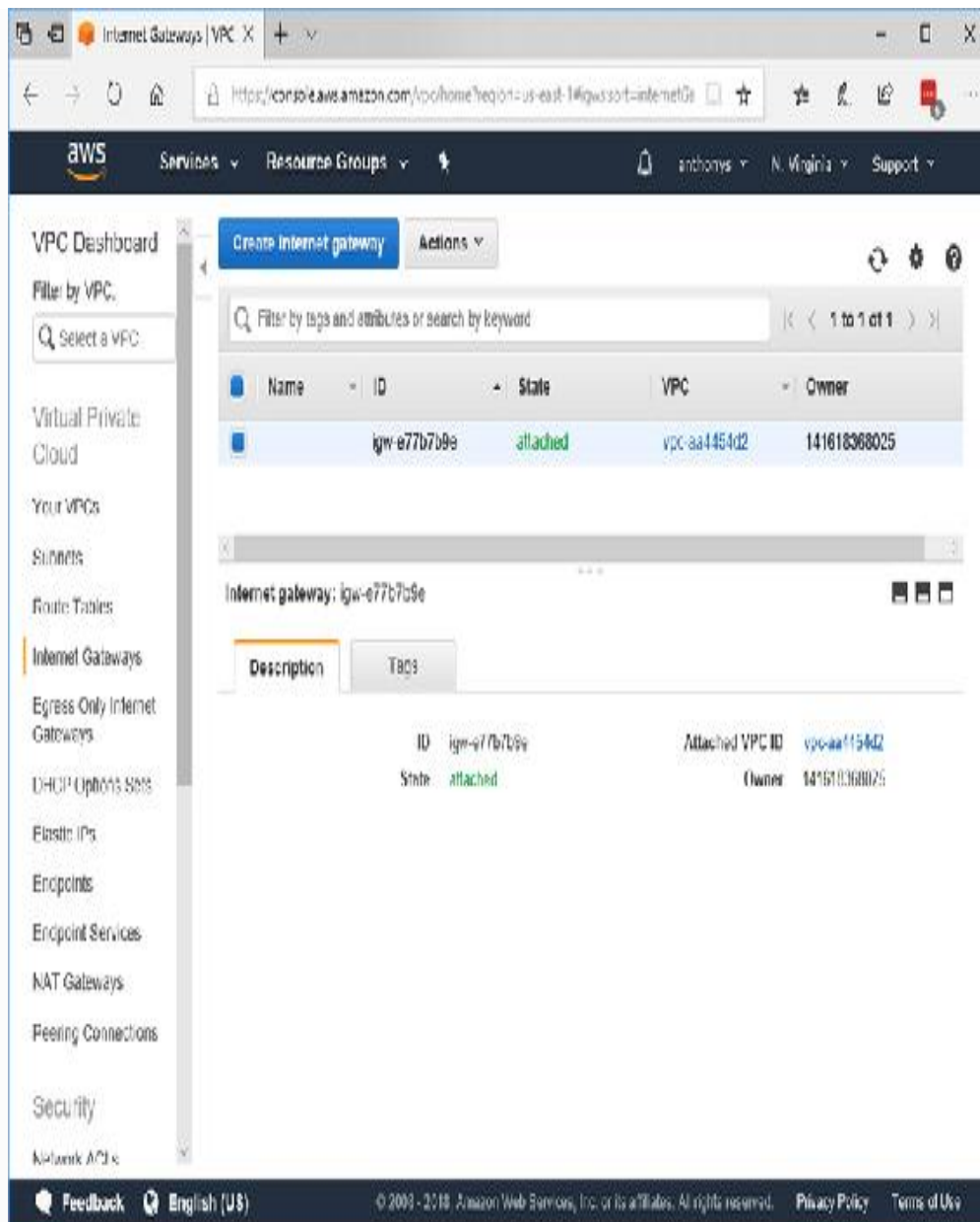


Figure 3-2 An Internet Gateway

- **NAT Gateway:** Translates your privately addressed VPC resources to access the Internet using public IP addresses.
- **NACLs:** Network access control lists allow you to control access to your VPC subnets; these are stateless constructs, meaning you must configure inbound and outbound rules,

as there is no automatic recognition of state with traffic flows and no automated access entries.

INTRODUCTION TO SECURITY GROUPS

Because security of your resources in the cloud is a prime concern for both you and Amazon, it is no big surprise that AWS provides you with built-in firewalls with your compute resources. These security groups help you easily control the accessibility of your EC2 resources, for example. Figure 3-3 shows an example of a security group in AWS.

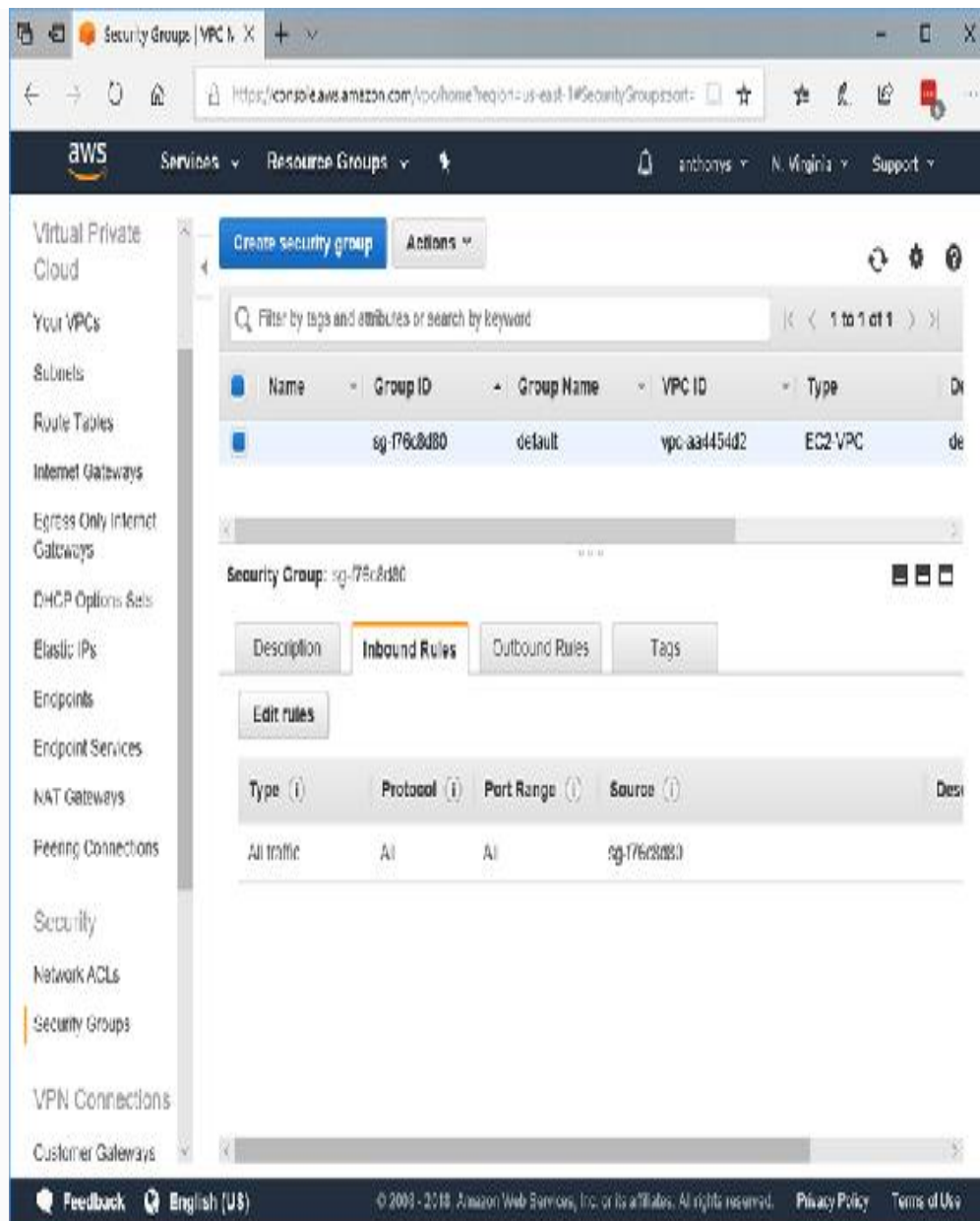


Figure 3-3 An AWS Security Group

Perhaps you have a Web tier in your AWS architecture. You can configure the security group for this tier to permit HTTP and HTTPS traffic from customers using the Web tier, while at the same time you can permit your team of support engineers to access the Web tier using SSH and RDP. All other protocol

attempts at accessing the Web tier are denied by the security group.

INTRODUCTION TO COMPUTE SERVICES

Because compute resources are so incredibly important to our IT solutions, it is no surprise that Amazon has many services that center around compute resources. Although the primary job of this section is to provide you with valuable information regarding the primary compute resource in AWS, Elastic Compute Cloud (EC2), you first need an understanding of the other compute resources available to you.



Lambda

AWS Lambda is an exciting alternative to EC2 instances that you must operate and maintain. Lambda provides compute resources in a fully managed (by AWS) serverless compute cloud. You send compute requirements to Lambda in a variety of different manners (such as a call from a Web app), and Lambda takes care of the compute requirements for you. Sub-second metering is used for your cost calculations, so quite often it is a very inexpensive way to provide the compute resources you require. It also supports many different programming languages to ease use. With Lambda, a typical workflow follows these steps:

1. You upload your code to AWS Lambda.
2. You set up your code to trigger from either other AWS services, HTTP endpoints, or in-app activity.
3. Lambda runs your code when triggered, only consuming the resources needed; it is important to realize that like most AWS services, Lambda provides continuous scaling, as needed.
4. You pay for just the compute time required.

Elastic Beanstalk

Elastic Beanstalk offers a very quick and simple method for getting your applications into the AWS Cloud. It is actually a Platform as a Service (PaaS) offering. The infrastructure and platform are quickly built for you in the cloud. This permits the quick deployment of your applications. Elastic Beanstalk also reduces the ongoing management complexity of your deployment. Importantly, you maintain control of the platform. For example, should you want to scale your applications more aggressively, you have complete control. Another great aspect to this service is that it supports a wide variety of languages and platforms, such as Go, Java SE, PHP, Python, and Node.js, just to name a few. Application upgrades are simple, as you just deploy them to Elastic Beanstalk as needed.

While it is easy to implement, it is also robust. You supply the application code, and AWS provides components such as the following:

- Application services

- HTTP services
- Required operating systems
- Required language interpreters
- The physical hosts required

EC2

Amazon Elastic Compute Cloud (EC2) is a web service that gives secure and resizable compute resources in the AWS Cloud. The EC2 service allows you to provision and configure capacity with minimal effort. It provides you with easy control of your computing resources.

EC2 reduces the time required to obtain and boot new servers (EC2 instances) to just minutes. This efficiency allows you to scale capacity vertically (up and down, making your server resources bigger or smaller) and horizontally (out and in, adding more capacity in the form of more instances), as your computing requirements change. As you might recall from previous chapters, this property is known as *elasticity*.

The many benefits of EC2 in AWS include the following:

- EC2 allows for controlled expenditures as your business expands; you pay only for the resources you use as your business grows.
- EC2 provides you with the tools to build failure-resilient applications that isolate themselves from common failure scenarios.

- EC2 enables you to increase or decrease capacity within minutes, not hours or days. You can commission one, hundreds, or even thousands of server instances simultaneously.
- You have complete control of your EC2 instances. You have root access to each one, and you can interact with them as you would any traditional virtual machine.
- You can stop your EC2 instance while retaining the data on your boot partition and then subsequently restart the same instance using web service APIs. Instances can be stopped and started remotely using web service APIs.
- You can choose among multiple instance types, operating systems, and software packages. Instance types inside AWS permit the choice of emphasis on CPU, RAM, and/or networking resources.
- EC2 integrates with most AWS services, such as Simple Storage Service (S3), Relational Database Service (RDS), and Virtual Private Cloud (VPC). This tight integration allows you to use EC2 for a wide variety of compute scenarios.
- EC2 offers a reliable environment where replacement instances can be rapidly and predictably commissioned. The service runs within Amazon's proven network infrastructure and data centers. AWS offers as much as 99.95 percent availability for each region.
- Amazon EC2 works in conjunction with Amazon VPC to provide security and robust networking functionality for

your compute resources:

- Your compute instances are located in a VPC with an IP address range that you specify.
- You decide which instances are exposed to the Internet and which remain private.
- Security groups and network access control lists (ACLs) allow you to control inbound and outbound access to and from your network interfaces.
- You can connect your existing IT infrastructure to resources in your VPC using industry-standard encrypted IPsec virtual private network (VPN) connections, or you can take advantage of a private AWS Direct Connect option.
- You can provision your Amazon EC2 resources as dedicated instances. Dedicated instances are Amazon EC2 instances that run on hardware dedicated to a single customer for additional isolation. Alternatively, you can provision your Amazon EC2 resources on dedicated hosts, which are physical servers with EC2 instance capacity entirely dedicated to your use. Dedicated hosts can help you address compliance requirements and reduce costs by allowing you to use your existing server-bound software licenses.



Several pricing models exist, including the following:

- **On-demand instances:** With this model, you pay for compute capacity by the hour (or even by the second with some AMIs) with no long-term commitments. You can increase or decrease your compute capacity depending on the demands of your application and pay the specified hourly rate only for the instances you use. The use of on-demand instances frees you from the costs and complexities of planning, purchasing, and maintaining hardware. As mentioned in the first section, this model also transforms what are commonly substantial fixed costs into much smaller variable costs.
- **Reserved instances:** This model provides you with a significant discount (up to 75 percent) compared to on-demand instance pricing. You have the flexibility to change families, operating system types, and tenancies while benefitting from reserved instance pricing when you use convertible reserved instances. Figure 3-4 shows the beginning steps of configured reserved instances in AWS.

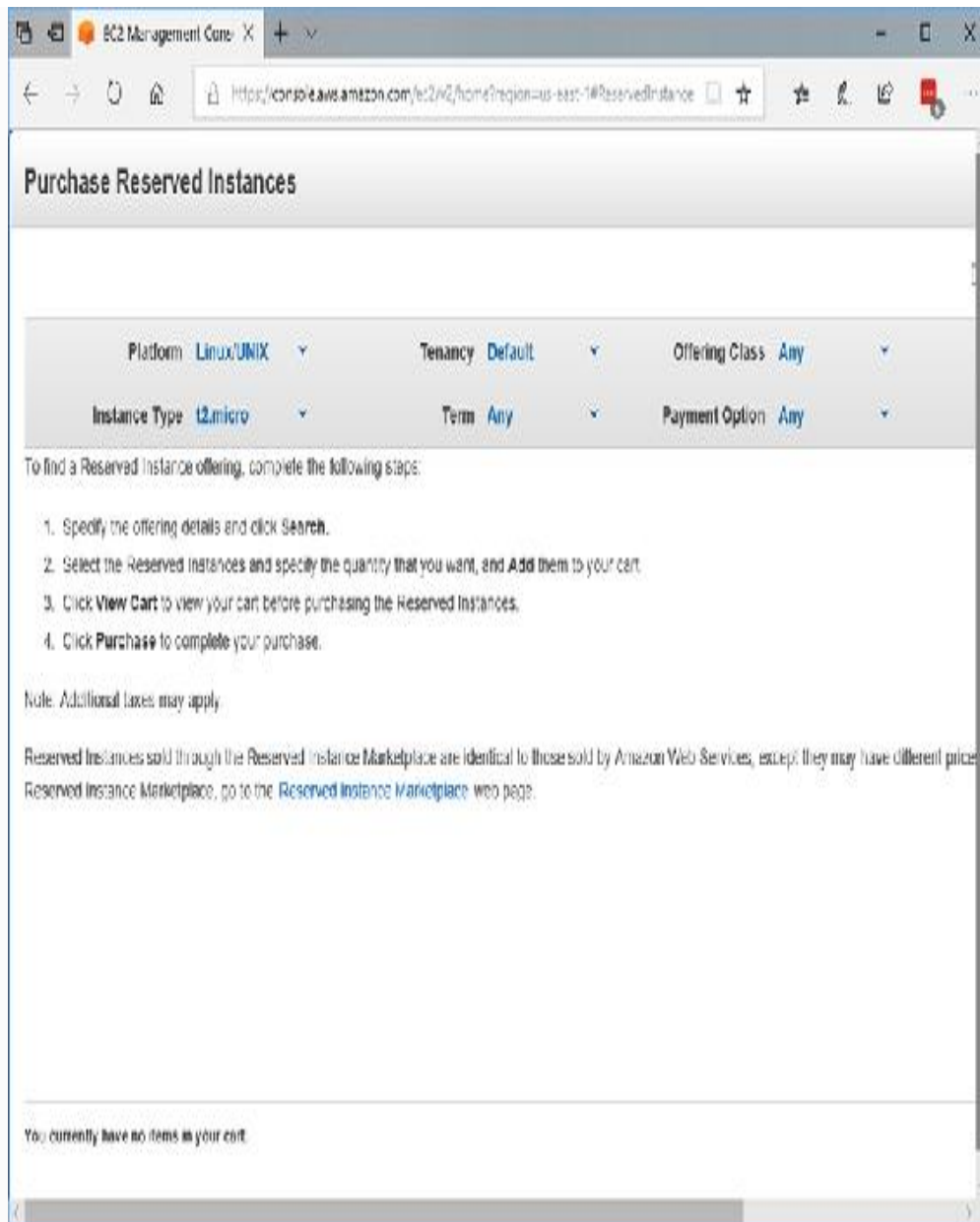


Figure 3-4 Purchasing Reserved Instances in AWS

- **Spot instances:** These instances allow you to bid on spare EC2 computing capacity. Because spot instances are often available at a discount compared to on-demand pricing, you can significantly reduce the cost (up to 90 percent) of running your applications.

INTRODUCTION TO EBS

Amazon Elastic Block Store (Amazon EBS) provides persistent block storage volumes for use with EC2 instances in the AWS Cloud. Each Amazon EBS volume is automatically replicated within its Availability Zone to protect you from component failure, offering high availability and durability.

EBS volumes offer the consistent and low-latency performance needed to run your workloads. With Amazon EBS, you can scale your usage up or down within minutes—all while paying a low price for only what you provision.

Features of EBS include the following:

- **High-performance volumes:** Choose between solid-state disk (SSD)-backed or hard disk drive (HDD)-backed volumes that can deliver the performance you need for your most demanding applications.
- **Availability:** Each Amazon EBS volume is designed for 99.999 percent availability and automatically replicates within its Availability Zone to protect your applications from component failure.
- **Encryption:** Amazon EBS encryption provides seamless support for data at rest and data in transit between EC2 instances and EBS volumes.
- **Access management:** Amazon's flexible access control policies allow you to specify who can access which EBS volumes, ensuring secure access to your data.

- **Snapshots:** You can protect your data by creating point-in-time snapshots of EBS volumes, which are backed up to Amazon S3 for long-term durability.

INTRODUCTION TO S3

Amazon Simple Storage Service (Amazon S3) is object storage with a simple web service interface to store and retrieve any amount of data from anywhere on the web. It is designed to deliver 99.999999999 percent durability. Figure 3-5 shows two storage buckets in S3.

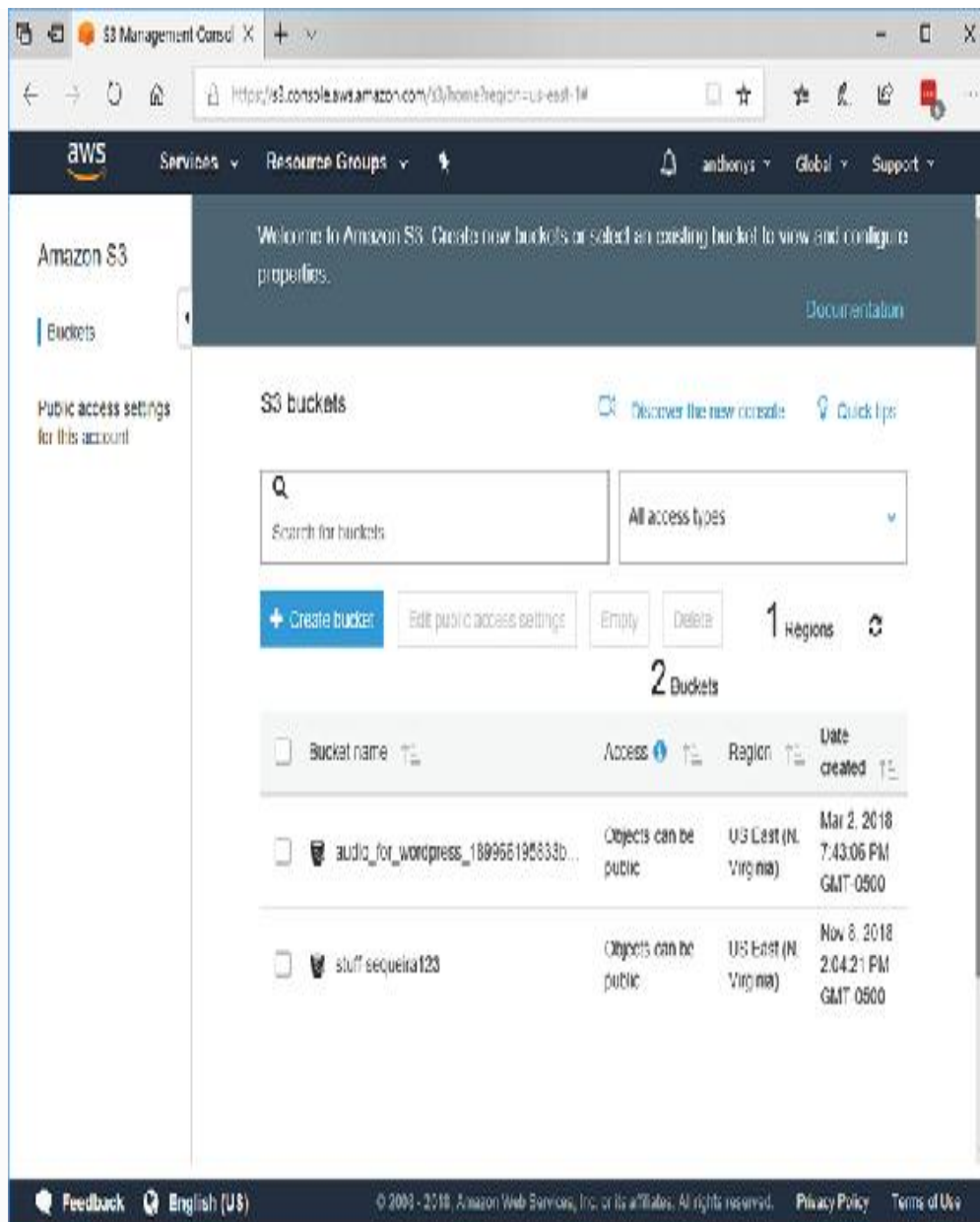


Figure 3-5 AWS S3

You can use Amazon S3 for a vast number of purposes, such as the following:

- Primary storage for cloud-native applications
- A bulk repository, or “data lake,” for analytics

- A target for backup and recovery and disaster recovery
- For use with serverless computing

You can move large volumes of data into or out of Amazon S3 with Amazon's cloud data migration options. You can store data in S3 and then automatically tier the data into lower-cost, longer-term cloud storage classes like S3 Standard–Infrequent Access and Glacier for archiving. You could even utilize a new storage class that reduces high availability (One Zone Infrequent Access) when you do not require it and want to save on storage costs.



S3 offers many advantages, including the following:

- **Simple:** S3 is easy to use with a web-based management console and mobile app. Amazon S3 also provides full REST APIs and SDKs for easy integration with third-party technologies. A command-line interface (CLI) is also extremely popular for working with S3.
- **Durable:** S3 provides a durable infrastructure to store essential data. Amazon designed S3 for durability of 99.999999999 percent of objects. S3 redundantly stores your data across multiple facilities and multiple devices in each facility.
- **Scalable:** With S3, you can store as much data as you want and access it when needed. While there is a 5TB limit on

the size of an individual object, there is no limit to the number of objects you can store!

- **Secure:** S3 supports data transfer over SSL and automatic encryption of your data following the upload. If you want, you can control client-side or server-side encryption. You can use Amazon-generated or customer-generated keys and have full key management capabilities/options. You can also configure bucket policies to manage object permissions and control access to your data using Identity and Access Management (IAM).
- **Available:** S3 Standard is designed for up to 99.99 percent availability of objects over a given year and is backed by the Amazon S3 service level agreement, ensuring that you can rely on it when needed. You can also choose an AWS region to optimize for latency, minimize costs, or address regulatory requirements.
- **Low cost:** S3 allows you to store large amounts of data at a small cost. Using lifecycle policies, you can configure the automatic migration of your data to different storage tiers within AWS.
- **Simple data transfer:** Amazon provides multiple options for cloud data migration and makes it simple and cost-effective for you to move large volumes of data into or out of S3. You can choose from network-optimized, physical disk-based, and third-party connector methods for import to or export from S3.
- **Integrated:** S3 is deeply integrated with other AWS services to make it easier to build solutions that use a range

of AWS services. Integrations include the following:

- CloudFront
 - CloudWatch
 - Kinesis
 - Relational Database Service (RDS)
 - Glacier
 - Elastic Block Store (EBS)
 - DynamoDB
 - Redshift
 - Route 53
 - Elastic MapReduce (EMR)
 - Virtual Private Cloud (VPC)
 - Key Management Service (KMS)
 - Lambda
- **Easy to manage:** S3 storage management features allow you to take a data-driven approach to storage optimization, data security, and management efficiency. These enterprise-class capabilities give you data about your data so that you can manage your storage based on that personalized metadata.

While technically part of the S3 service, Amazon Glacier is a secure, durable, and extremely low-cost storage service for data archiving and long-term backup. With Glacier, you can do the following:

- Reliably store large or small amounts of data for as little as \$0.004 per gigabyte per month.
- Save money compared to on-premises storage options.
- Keep costs low yet suitable for varying retrieval needs.
- Choose from three options for access to archives—from a few minutes to several hours.

INTRODUCTION TO AWS DATABASE SOLUTIONS

Many types of databases are available today. The great news is that AWS supports these varieties. In fact, AWS permits several different approaches to their implementation. This section gives you an overview of these exciting technologies.



Aurora

Amazon Aurora is a MySQL- and PostgreSQL-compatible relational database engine. It offers many benefits, including the following:

- **High performance:** Aurora can provide up to five times the throughput of standard MySQL or twice the throughput of standard PostgreSQL running on the same hardware.
- **Highly secure:** Aurora provides multiple levels of security for your database. These include network isolation using a VPC, encryption of data at rest using keys you create and

control through Key Management Service (KMS), and encryption of data in transit using SSL.

- **MySQL and PostgreSQL compatible:** The Aurora database engine is fully compatible with MySQL 5.6 and MySQL 5.7 using the InnoDB storage engine.
- **Highly scalable:** You can scale your Aurora database from an instance with two vCPUs and 4 GiB of memory up to an instance with 32 vCPUs and 244 GiB of memory.
- **High availability and durability:** Aurora is designed to offer higher than 99.99 percent availability. It is also amazing when it comes to durability, ensuring six synchronous copies of your data running across three AZs. This becomes a huge advantage over standard RDS implementations.
- **Fully managed:** Aurora is a fully managed database service. Amazon handles tasks such as hardware provisioning, software patching, setup, configuration, monitoring, and backups.



Relational Database Service

Relational Database Service (RDS) makes it easy to set up, operate, and scale a relational database in the cloud. RDS provides six database engines to choose from: Aurora, PostgreSQL, MySQL, MariaDB, Oracle, and Microsoft SQL Server.

Benefits of RDS include the following:

- **Fast and easy to administer:** You can use the AWS Management Console, the AWS RDS command-line interface, or simple API calls to access the capabilities of a production-ready relational database in minutes.
- **Highly scalable:** You can scale your database's compute and storage resources with only a few mouse clicks or an API call, often with no downtime.
- **Available and durable:** RDS runs on the same highly reliable infrastructure used by other Amazon Web Services. When you provision a Multi-AZ DB instance, RDS synchronously replicates the data to a standby instance in a different Availability Zone (AZ).
- **Secure:** RDS makes it easy to control network access to your database. RDS also lets you run your database instances in a VPC, which enables you to isolate your database instances and connect to your existing IT infrastructure through an industry-standard encrypted IPsec VPN. Many RDS engine types offer encryption at rest and encryption in transit. You can also take advantage of Direct Connect.
- **Inexpensive:** You pay low rates and only for the resources you consume.

DynamoDB

Amazon DynamoDB is a fast and flexible NoSQL database service for all applications that need consistent, single-digit

millisecond latency at any scale. It is a great fit for mobile, web, gaming, ad-tech, Internet of Things (IoT), and many other applications.

Benefits of DynamoDB include the following:

- **Fast, consistent performance:** DynamoDB delivers consistent, fast performance at any scale for all applications.
- **Highly scalable:** When you create a table, you specify how much request capacity you require. If your throughput requirements change, you update your table's request capacity using the AWS Management Console or the DynamoDB APIs. DynamoDB manages all the scaling behind the scenes, and you are still able to achieve your previous throughput levels while scaling is underway. Instant scaling and auto-scaling capabilities now exist that even assist you if you are unsure of the initial capacity you require.
- **Fully managed:** DynamoDB is a fully managed cloud NoSQL database service. You create a database table, optionally set your throughput or allow auto-scaling, and let the service handle the rest.
- **Event-driven programming:** DynamoDB integrates with Lambda to provide triggers that enable you to architect applications that automatically react to data changes.
- **Fine-grained access control:** DynamoDB integrates with IAM for fine-grained access control.

- **Flexible:** DynamoDB supports both document and key-value data structures, giving you the flexibility to design the best data architecture that is optimal for your application.

ElastiCache

ElastiCache is a web service that makes it easy to deploy, operate, and scale an in-memory cache in the cloud. The service improves the performance of web applications by allowing you to retrieve information from fast, managed, in-memory caches, instead of relying entirely on slower disk-based databases.

ElastiCache supports two open-source in-memory caching engines:

- **Redis:** A fast, open-source in-memory data store and cache. ElastiCache for Redis is a Redis-compatible in-memory service that delivers the ease of use and power of Redis along with the availability, reliability, and performance suitable for the most demanding applications.
- **Memcached:** A widely adopted memory object caching system. ElastiCache is protocol-compliant with Memcached, so tools that you use today with existing Memcached environments work seamlessly with the service.

Redshift

Redshift is a fast, fully managed, petabyte-scale data warehouse that makes it simple and cost-effective to analyze all your data using your existing business intelligence tools.

Features include the following:

- High query performance on data sets ranging in size from a hundred gigabytes to a petabyte or more.
- Using columnar storage, data compression, and zone maps to reduce the amount of I/O needed to perform queries.
- Redshift has massively parallel processing (MPP) data warehouse architecture, parallelizing and distributing SQL operations to take advantage of all available resources. The underlying hardware is designed for high-performance data processing, using locally attached storage to maximize throughput between the CPUs and drives, and a 10GigE mesh network to maximize throughput between nodes.

Database Migration Service

AWS Database Migration Service helps you migrate databases to or from AWS easily and securely. Features include the following:

- The source database remains fully operational during the migration, minimizing downtime to applications that rely on the database.
- It migrates your data to and from most widely used commercial and open-source databases. The service supports homogeneous migrations such as Oracle to Oracle, as well as various migrations between different

database platforms, such as Oracle to Amazon Aurora or Microsoft SQL Server to MySQL.

- It also allows you to stream data to Redshift from any of the supported sources, including Aurora, PostgreSQL, MySQL, MariaDB, Oracle, SAP ASE, Teradata, and SQL Server, enabling consolidation and straightforward analysis of data in the petabyte-scale data warehouse.
- You can use AWS Database Migration Service for continuous data replication with high availability.

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the exercises here, [Chapter 16, “Final Preparation,”](#) and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. [Table 3-2](#) lists these key topics and the page numbers on which each is found.



Table 3-2 Key Topics for [Chapter 3](#)

Key Topic Element	Description	Page Number
List	Components of the Global Infrastructure	
List	Features of VPCs	
Overview	Lambda	
List	Instance types	
List	Advantages of S3	
Overview	Aurora	
Overview	RDS	

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

Networking and content delivery

regions

Availability Zones

Edge Locations

security groups

on-demand instances

reserved instances

spot instances

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. Name the three pricing models for EC2.
2. Name the three main components of the Global Infrastructure.
3. What two types of database compatibility options exist in RDS?

Chapter 4

Cloud Architecture Design Principles

This chapter covers the following subjects:

- **The Well-Architected Framework:** AWS does not just hope you can architect a brilliant design on their cloud; they provide you detailed guidance on how to do so. “The AWS Well-Architected Framework” is a thorough document that is detailed in this section of the chapter.
- **Fault Tolerance and High Availability:** This section discusses the relative ease of achieving a fault tolerant and highly available architecture in AWS.
- **Web Hosting:** This section of the chapter describes how AWS can assist dramatically in the hosting of various web application content.

There are many techniques and approaches to services of AWS that have been tried successfully by many companies all over the world. In this chapter, you benefit from all this experimentation and learn some of the key design principles that can guide you throughout your AWS experiences.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. [Table 4-1](#) lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 4-1 “Do I Know This Already?” Foundation Topics
Section-to-Question Mapping

Foundations Topics Section	Questions
The Well-Architected Framework	1-2
Fault Tolerance and High Availability	3-4
Web Hosting	5-6

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following is not one of the pillars of “[The Well-Architected Framework](#)” from Amazon?

- a.** Cost optimization
 - b.** Security
 - c.** Operational excellence
 - d.** Speed
- 2.** Ensuring that you have “traceability” is critical in AWS.
This is typically under what AWS design pillar?
 - a.** Cost optimization
 - b.** Operational excellence
 - c.** Performance efficiency
 - d.** Security
- 3.** Which of the following is true regarding HA in your on-premises data center?
 - a.** It is typically only reserved for the most mission-critical systems or data.
 - b.** It is typically implemented at a lower cost than cloud.
 - c.** It is typically implemented throughout the entire data center.
 - d.** It is never truly achievable.
- 4.** Which is not a typical service or tool associated with HA in AWS?
 - a.** Auto Scaling
 - b.** ELB
 - c.** CloudWatch

- d. CloudTrail
- 5. What is the DNS service offered by AWS?
 - a. SQS
 - b. Route 53
 - c. CloudFront
 - d. CloudFormation
- 6. Where should firewalling be accomplished in your web hosting design in AWS?
 - a. At the perimeter
 - b. At the core
 - c. Everywhere
 - d. For all access layer functions

FOUNDATION TOPICS

THE WELL-ARCHITECTED FRAMEWORK

You might think that at Amazon, really smart engineers sat down to pen “The Well-Architected Framework” based on their experience with cloud design. This is only partially true. In order to provide you with a document as critical as “The Well-Architected Framework,” these engineers and architects also did something very smart. They analyzed the actual implementations of successful designs by some of their largest and most successful customers (with their permission of

course). All of this research gave rise to the framework that we cover here.

What are some of the goals of “The Well-Architected Framework”? Well, they are pretty lofty. They include designing for security, performance, resiliency, and efficiency. The framework also provides you with the valuable opportunity to evaluate a proposed design against the tried and true principles contained in the document. This makes it an even more valuable tool.

Amazon had many goals when they created this framework. Here are the most important:

- Build and deploy solutions faster than ever before.
- Lower and mitigate the risks associated with a move to the cloud.
- Make informed decisions about how to implement solutions in the cloud.
- Learn the most powerful best-practice approaches to using AWS services and tools.



To help organize the framework and make it more valuable, Amazon focused the framework around the following five pillars:

- Operational excellence
- Security

- Reliability
- Performance efficiency
- Cost optimization

We should examine each of these pillars and the important design concepts in each.

Operational Excellence

The overall objective of this pillar is to make sure you run and monitor systems to ensure that they are providing value for the business goals of the organization.

Note

It is very important that you keep this point in mind. While so many of us in technology find the cloud incredibly “cool,” we should never be targeting technology just because it is very clever and exciting; instead, we should be targeting technology because it assists our organization in achieving the most important business objectives.



This pillar consists of the following important design principles:

- Perform operations in code.
- Annotate documentation as much as possible.
- Make frequent small and reversible changes to the architecture in order to improve it.

- Refine your operational procedures frequently in order to improve them.
- Anticipate failures and have your recovery plans in place.
- Learn from any failures that you might have in your architecture in AWS.

Security

Clearly, the job of this pillar is to help protect your assets, your systems, and your information associated with AWS. This pillar should also assist you with risk assessments and your mitigation practices.



This pillar consists of the following important design principles:

- You should use strong identity practices in your architecture.
- There should be full traceability in all operations.
- Security should be implemented in absolutely all layers of your architecture.
- There should be a concerted effort to automate as many of the security best practices as possible.
- Information should be secured at rest as well as in transit.
- You should prepare as much as possible for the inevitable security events in your architecture and cloud.

Reliability

This pillar consists of many important design principles that all center around ensuring your design can easily recover from service failures. It also ensures your architecture can grow resources as needed on-demand. Reliability in the cloud also means that disruptions can be mitigated with relative ease.



Here are the design goals around this pillar:

- Test recovery.
- Automate failure recovery as much as possible.
- Automatically scale horizontally when needed.
- Stop guessing at capacity for IT resources.
- Manage changes through automation.

Performance Efficiency

This pillar concerns itself with the use of AWS resources as efficiently as possible. The efficiency should be maintained as demand changes and technology evolves.



Here are the design goals around this pillar:

- Democratize advanced technologies—meaning make them available to the masses.

- Take resources globally in minutes.
- Target serverless computing as much as possible.
- Experiment freely and often.
- Maintain mechanical sympathy—meaning match business goals to the appropriate technologies.

Cost Optimization

The goal of this pillar is quite simple—to save money and stop the wasting of investments in technology.



The design goals are also straightforward:

- Adopt a consumption model; this emphasizes the OpEx approach to IT.
- Measure the efficiency of your architecture closely.
- Stop spending money needlessly in an attempt to solve IT problems.
- Closely analyze the expenditures in your AWS implementation.
- Use managed services as much as possible.

FAULT TOLERANCE AND HIGH AVAILABILITY

Let's begin by ensuring you understand these two critical concepts. Fault tolerance (FT) refers to the ability of a system to sustain the loss of a component without occurring any downtime at all. High availability (HA) refers to the ability of your entire architecture to maintain an increased level of availability. You should note that fault tolerance is a subcomponent of high availability.

There are two important considerations for high availability with AWS. First, the HA should be able to be achieved at a small fraction of the cost of achieving HA in a traditional data center approach on your premises. Second, the HA should be achievable with a minimum of human intervention. In fact, most consider HA to mean there is *no* human intervention.

Understand that when you try and implement HA on premises using traditional IT technology, it tends to be very expensive. It also tends to only protect the most mission-critical resources. In AWS, HA tends to be much more cost effective and much more comprehensive for the entire architecture.



What are some of the key services and tools of AWS that make incredible levels of HA possible?

- Elastic Load Balancers
- Elastic IP Addresses
- Route 53
- Auto Scaling

- CloudWatch

What about the tools that exist in AWS specifically for the fault tolerance aspect of HA?

- Simple Queue Service (SQS)
- Simple Storage Service (S3)
- Simple DB

WEB HOSTING

Web hosting is a trend that began decades ago and shows no sign of slowing down. More and more applications are brought to users by being hosted by web servers. Web servers might play a key part in your organization for the following reasons:

- Hosting your company website
- Web-based Content Management Systems
- Social media applications
- Internal SharePoint sites
- Web services such as API endpoints



No matter your specific need for web hosting with AWS, you should be able to achieve the following compelling benefits:

- **Cost effectiveness:** Simple on-demand provisioning is needed as more web server scalability is needed.

- **On-demand resources:** This capability promotes the use of test fleets, staging servers, and simulated user traffic.

Architecturally, there are many positive effects, such as the following:

- An elimination of reliance on strict physical appliances.
- Firewalling can be done everywhere in the architecture.
- Multiple data centers can be located across the globe with ease.
- Hosts can be considered completely ephemeral and dynamic.

You can also take advantage of many services and tools of AWS that can aid you in your transition to the cloud. These include the following:

- VPC
- Route 53
- CloudFront
- Elastic Load Balancing
- AWS Web Application Firewall (WAF)
- AWS Shield
- Auto Scaling
- EC2
- ElastiCache
- RDS

- DynamoDB

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the exercises here, [Chapter 16, “Final Preparation,”](#) and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. [Table 4-2](#) lists a these key topics and the page numbers on which each is found.



Table 4-2 Key Topics for [Chapter 4](#)

Key Topic Element	Description	Page Number
List	The five pillars	
List	Design goals for operational excellence	
List	Design goals for security	
List	Design goals for reliability	
List	Design goals for performance efficiency	
List	Design goals for cost optimization	
List	Services for IT and HA	
List	Positive effects of web hosting on AWS	

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

HA

FT

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

- 1.** Name the five pillars in “The Well-Architected Framework” of AWS.
- 2.** What is often considered a subcomponent of HA?
- 3.** What service is often used to build the web server itself in AWS, especially if this web server is to host complex, dynamic content?

Part II

Domain 2: Security

Chapter 5

The AWS Shared Responsibility Model

This chapter covers the following subjects:

- **Understanding the Shared Responsibility Model:** This part of the chapter introduces you to the overall definition of the Shared Responsibility model.
- **Amazon Responsibilities:** This section provides examples of Amazon's responsibilities for security in your AWS implementation.
- **Client Responsibilities:** This section provides examples of client responsibilities for securing the resources in AWS.

Whereas some organizations are hesitant to move to the cloud due to sometimes false fears that their security will suffer, other organizations embrace the opportunities for greatly enhanced security. One major reason this is a reality is the existence of the AWS Shared Responsibility model. This model helps us fully understand the security environment when we operate in AWS. This chapter makes this subject simple and provides excellent examples of the various parts of the model.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. [Table 5-1](#) lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 5-1 “Do I Know This Already?” Foundation Topics
Section-to-Question Mapping

Foundations Topics Section	Questions
Understanding the Shared Responsibility Model	1-3
Amazon Responsibilities	4
Client Responsibilities	5

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. The AWS Shared Responsibility model divides security responsibilities between which two parties?

- a.** The AWS customer
 - b.** The AWS partner
 - c.** The community cloud vendor
 - d.** AWS
- 2.** Client responsibilities will vary in the Shared Responsibility model based on what major factor?
 - a.** The number of AWS employees in the region used by the customer
 - b.** The amount of customer data intended for cloud storage
 - c.** Which services the customer chooses to use of AWS
 - d.** How much money the customer is willing to spend on support
- 3.** Which is not a common category of IT security controls in the AWS Shared Responsibility model?
 - a.** Inherited
 - b.** Deferred
 - c.** Customer specific
 - d.** Shared
- 4.** Which of the following is not an example of an Amazon responsibility in the AWS Shared Responsibility model?
 - a.** Physical security of the data center
 - b.** Cloud software

- c. Edge locations
 - d. IAM policies
5. Which of the following is not an example of a client responsibility in the AWS Shared Responsibility model?
- a. Data integrity authentication
 - b. Guest operating system
 - c. Virtualization software on the host
 - d. Customer data

FOUNDATION TOPICS

UNDERSTANDING THE SHARED RESPONSIBILITY MODEL



The AWS Shared Responsibility model is very simple. It divides the security responsibilities between two parties—the AWS customer (you!) and Amazon (AWS). The fact that you are no longer responsible for a massive portion of the security required for scalable data centers is a huge advantage. You can leverage the massive budgets of Amazon and their intense expertise.

The next two sections of this chapter provide examples of responsibilities in each part of the model. But for now, realize the Amazon responsibilities include the host operating system

and virtualization layer down to the physical security of the facilities in which the service operates. It is your (the customer's) responsibility to secure the guest operating system (including updates and security patches), application software, and the AWS network security group firewall. Be aware that the client responsibilities will vary depending on which services the client chooses to use. The client responsibilities further vary based on the level of integration of AWS services consumed and their IT infrastructure. Laws and regulations that must be followed will also vary.

As shown in Figure 5-1, AWS is considered “security of the cloud” and the customer's responsibility is considered “security in the cloud.”

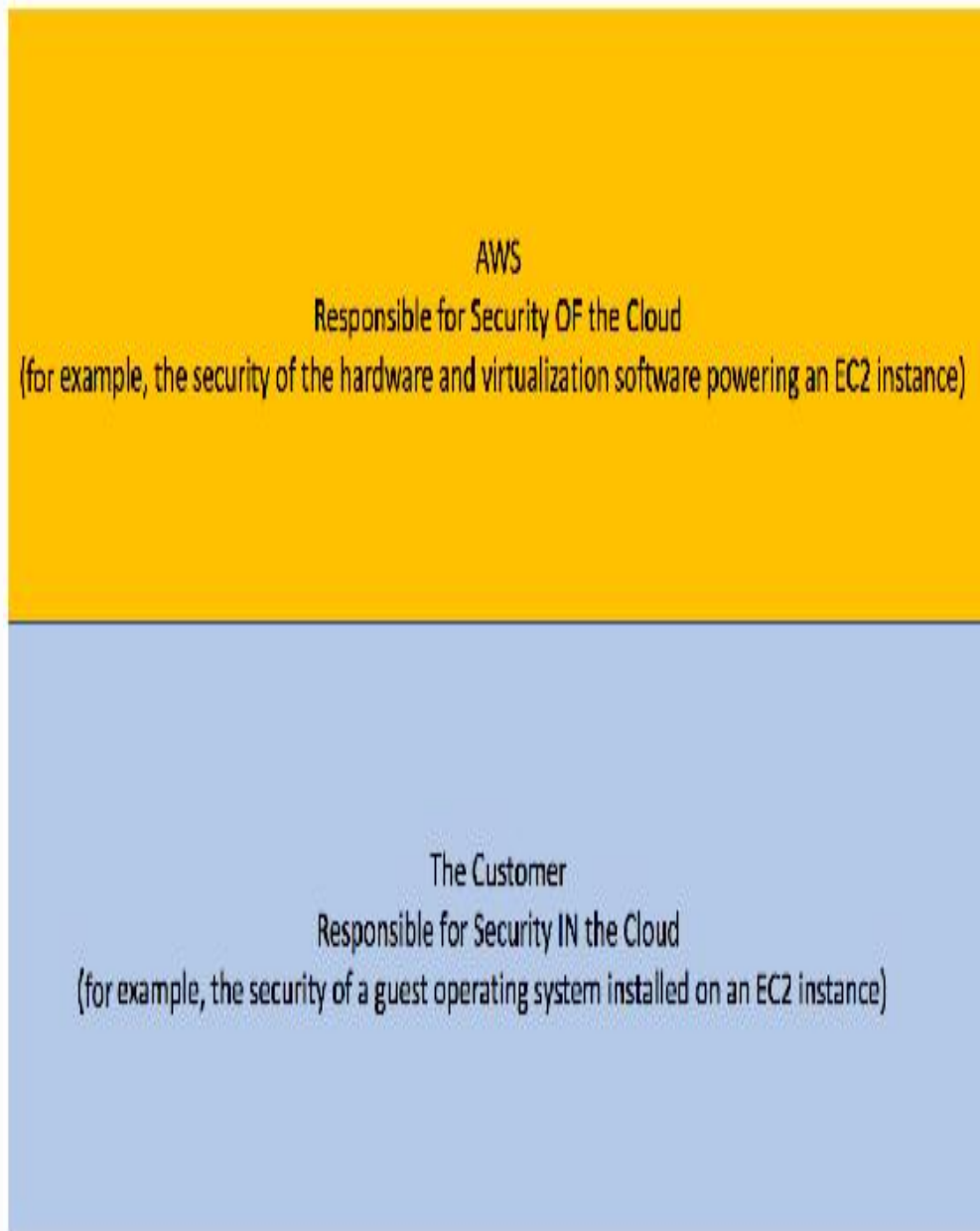


Figure 5-1 The AWS Shared Responsibility Model

In addition to partitioning the operational security concerns between the AWS client and AWS themselves, the Shared Responsibility model also applies to IT controls that are in use. Amazon categorizes these controls into three categories:

- **Inherited controls:** These are security controls the customer fully inherits from AWS. Perfect examples are the physical and environmental security controls used by Amazon.
- **Shared controls:** These are controls that apply to both the infrastructure layer of Amazon and the customer responsibilities. Note that these shared controls apply to each domain in completely separate contexts or perspectives. AWS provides the requirements for the infrastructure, and then the client must provide their own control implementation within their use of the services. A great example is Identity and Access Management (IAM). The IAM service must be secured, meet regulatory compliance, and function as intended, whereas the customer should create well-crafted policies.
- **Customer-specific controls:** These are security controls the customer is solely responsible for, and they vary based on the services the customer selects, of course. A great example would be when you apply specific patches to one of your operating systems on an EC2 instance.

AMAZON RESPONSIBILITIES

Remember, Amazon is considered responsible for security *of* the cloud. AWS is responsible for protecting the infrastructure that runs the services chosen. This includes the hardware and software required to power the AWS service as well as the networking and facilities used.



Specific Amazon responsibilities would include the following:

- Cloud software, including compute, storage, networking, and database software
- Hardware
- AWS Global Infrastructure, including regions, Availability Zones, and Edge Locations

CLIENT RESPONSIBILITIES

Remember, the client is considered responsible for security *in* the cloud. The specific services selected will cause variations in the client responsibilities. For example, if you are relying heavily on Simple Storage Service (S3) for storage, you will be responsible for knowledge and proper configuration of the security permissions for your resources. Another example would be if the client chooses to use EC2 and run an operating system like Windows Server 2016. The client is required to keep the operating system updated and patched and is also responsible for the application software they require on this guest operating system. The client is responsible for the appropriate security group configuration for the EC2 instance as well.



Specific examples of client responsibilities would include the following:

- Customer data
- Platform, applications, IAM
- Guest operating systems
- Network and firewall configurations
- Client-side data encryption
- Server-side encryption (file system and/or data)
- Networking traffic protection (encryption, integrity, and identity)

Figure 5-2 shows an example of a customer checking the security group settings that would apply to an EC2 instance. This is a perfect example of client responsibilities. AWS is responsible for making sure the security group functions as intended, but it is the client's responsibility to configure it correctly.

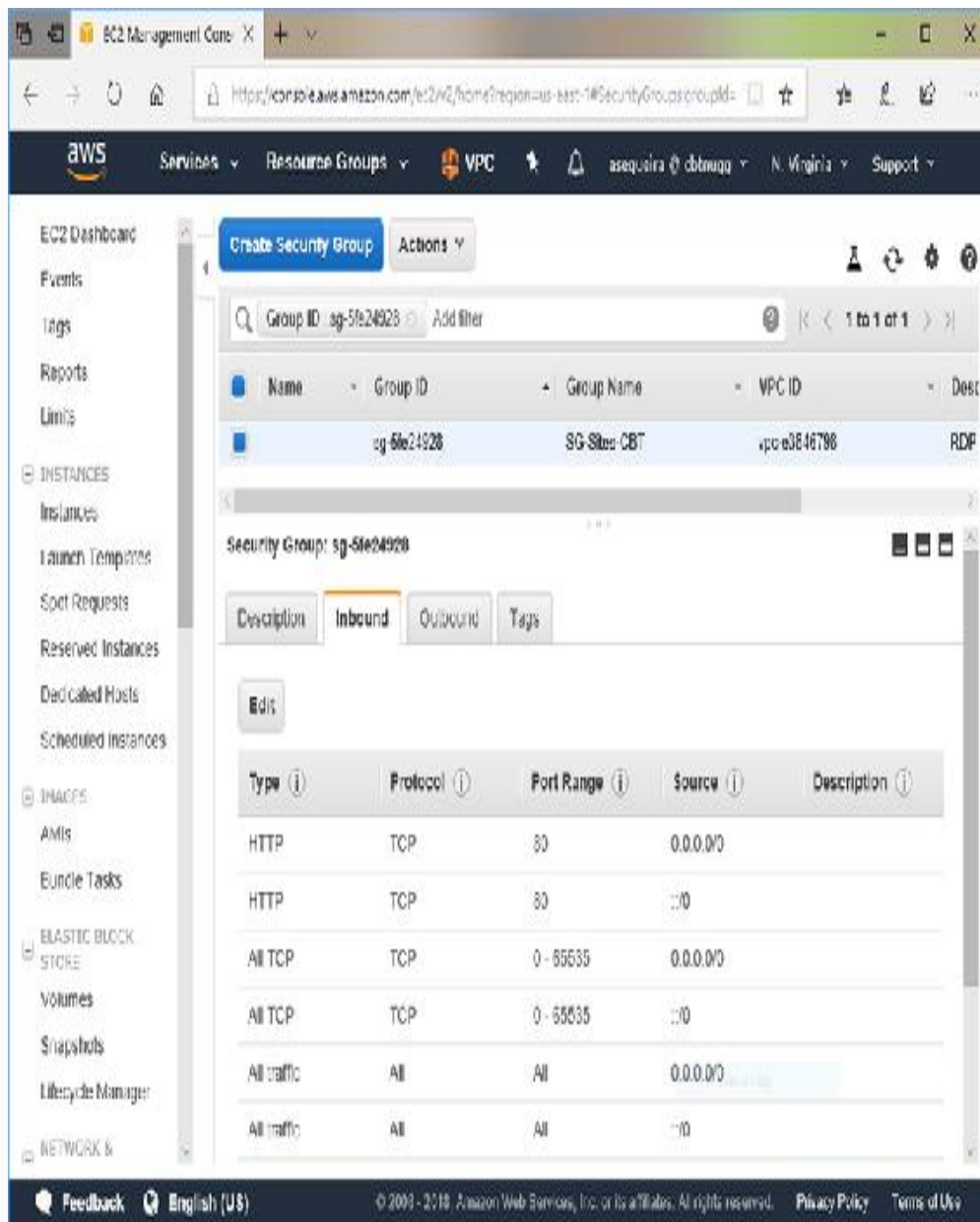


Figure 5-2 Checking the Security Group Settings for an EC2 Instance

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the

exercises here, Chapter 16, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 5-2 lists these key topics and the page numbers on which each is found.



Table 5-2 Key Topics for Chapter 5

Key Topic Element	Description	Page Number
Overview	The AWS Shared Responsibility model	
List	Examples of client responsibilities	
List	Examples of Amazon responsibilities	

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

The AWS Shared Responsibility model

security of the cloud

security in the cloud

Q&A

The answers to these questions appear in [Appendix A](#). For more practice with exam format questions, use the Pearson Test Prep Software Online.

- 1.** What would be an example of IT security controls that a customer inherits from Amazon?
- 2** Provide at least three examples of client responsibilities under the AWS Shared Responsibility model.
- 3** Provide at least two examples of Amazon responsibilities under the AWS Shared Responsibility model.

Chapter 6

Cloud Security and Compliance

This chapter covers the following subjects:

- **An Introduction to AWS Security:** This section discusses the major aspects of the AWS approaches to securing your infrastructure and resources.
- **AWS Security Compliance Programs:** This section of the chapter ensures you understand the many efforts that AWS engages in to ensure you can maintain compliance in security with laws and regulations you might face.

It is important that you understand the approaches that Amazon takes to security when it comes to AWS. It is also important to know specifics regarding the levels of compliance and attestation that AWS believes are important. This chapter discusses these points in detail, providing specific technologies that AWS uses to help ensure you can create the most secure architecture possible in the cloud and beyond.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. Table 6-1 lists the major

headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in Appendix A.

Table 6-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions
An Introduction to AWS Security	1-2
AWS Security Compliance Programs	3-4

1. Amazon is interested in offering you high levels of confidentiality with your data in AWS. What is a key technology area that accommodates this?
 - a. Authentication
 - b. Hashing
 - c. Encryption
 - d. Fault tolerance
2. What service in AWS assists your security efforts using roles, users, and groups?
 - a. S3
 - b. IAM
 - c. EC2

- d. Glacier
3. Amazon seeks out attestations from organizations that are what? (Choose two.)
- a. Dependent
 - b. Independent
 - c. Third party
 - d. Subsidiary
4. Which of the following is not something Amazon typically provides to AWS customers in the area of compliance?
- a. Mapping documents
 - b. Compliance playbooks
 - c. Security features
 - d. Physical host security playbooks

FOUNDATION TOPICS

AN INTRODUCTION TO AWS SECURITY

Amazon understands that a major concern for many organizations considering a move to public (or hybrid) clouds is security. As a result, they have taken great pains to ensure incredible levels of potential security for your organization. This includes massive efforts around confidentiality, integrity,

and *availability* (CIA). This is known as the “security triad” and is depicted in Figure 6-1.

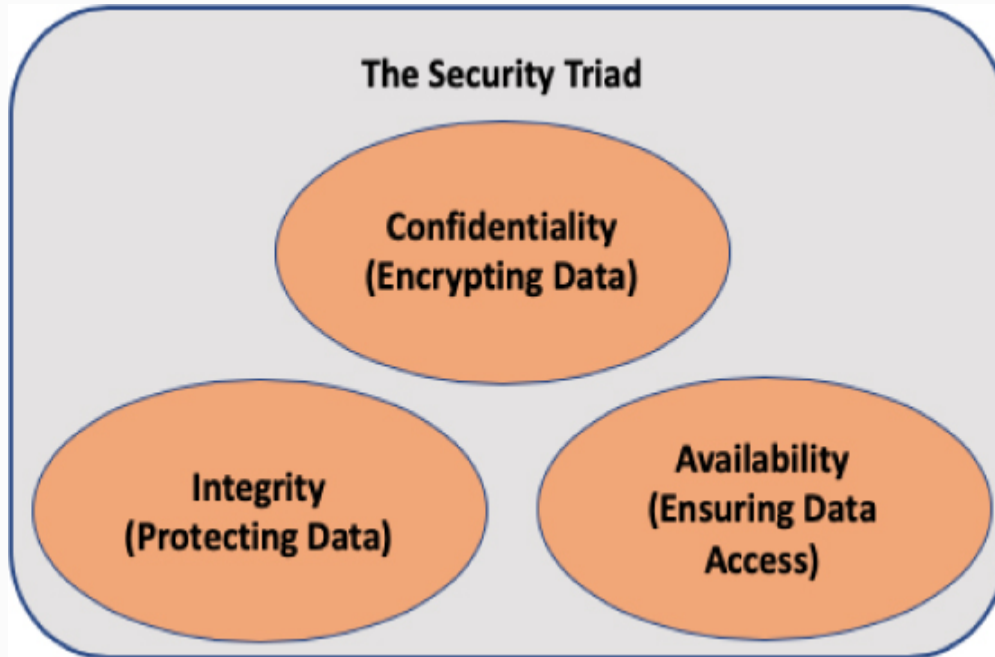


Figure 6-1 The Security Triad

What are some of the main approaches that Amazon takes to secure AWS? Let’s cover those now.

The first is keeping customer data as safe as possible. Amazon ensures a resilient and highly available infrastructure. High levels of the latest security technologies are deployed, and strong safeguards are in place for every aspect of Amazon’s security responsibilities.

With AWS, you can take advantage of rapid innovations in security technology at scale. This includes a robust Identity and Access Management (IAM) system, encryption of data at

rest and in transit, and segmentation services. Figure 6-2 shows the IAM components in AWS.

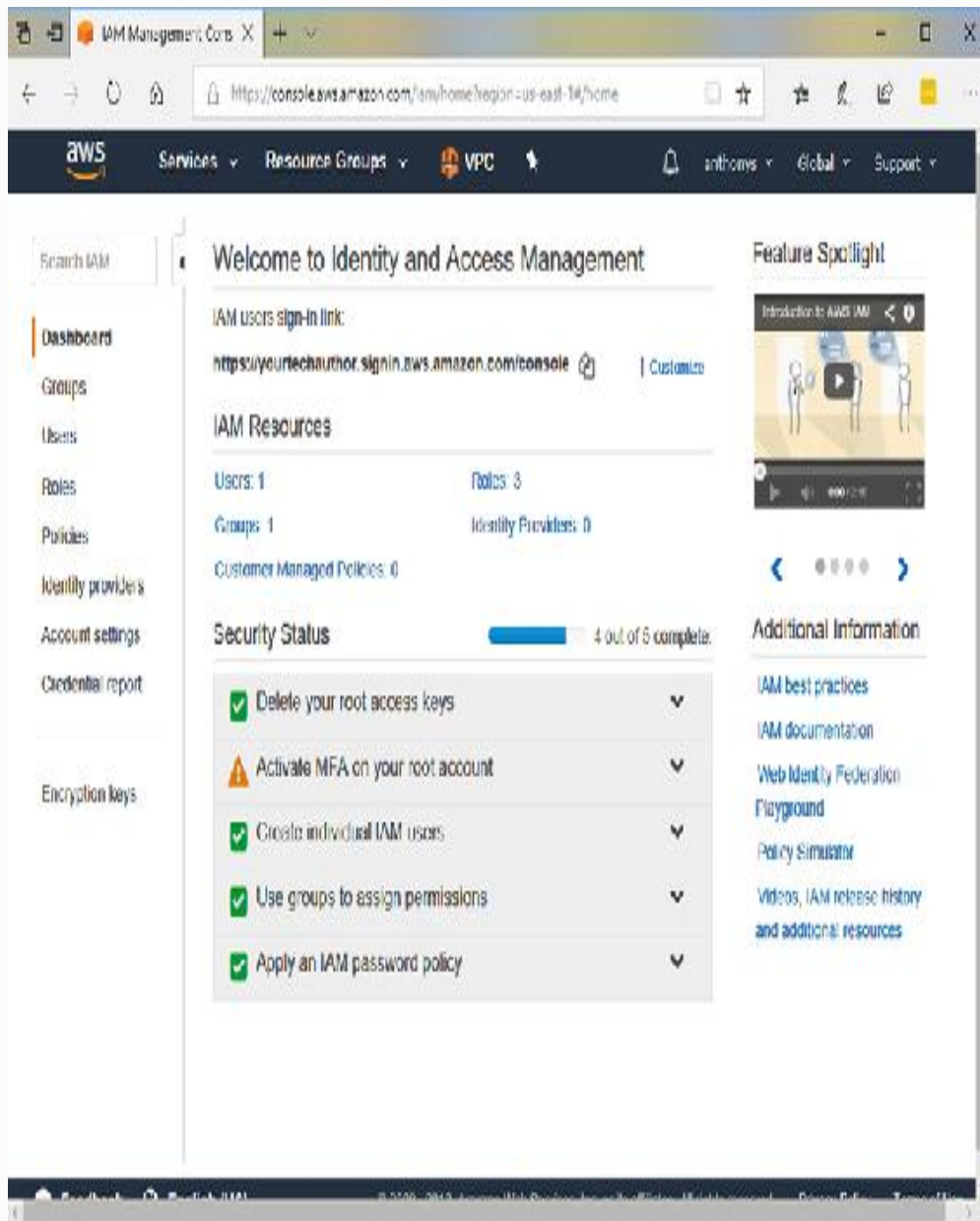


Figure 6-2 IAM in AWS

With AWS security, you pay for what you need. This permits high levels of security with controlled and elastic capacity and

costs.

AWS also ensures diverse compliance support to offer adherence to governance, oversight, and automation.

In addition, AWS follows a shared responsibility model that divides responsibility (clearly) between the customer (you) and Amazon. You can leverage their incredible expertise in secure infrastructures and technology knowledge. However, you must have expertise in securing components within AWS services. For example, you would be responsible for patching some of your virtual machine (EC2) deployments.

Note

The hardware on which your virtual machines reside is kept highly secure by Amazon.



Specific security products and features encompass a variety of tools and monitoring resources, including the following:

- **Robust network security:** Built-in firewalling, encryption in transit, private connectivity options, and built-in DDoS mitigation.
- **Efficient security tools:** Management of resource commissions and decommissions, inventory and configuration management tools, and best practice template definitions.

- **Data encryption at every level:** This includes database systems, key management, hardware-based storage options, and API support (like everything in AWS).
- **Access control and management:** Identity and Access Management, multifactor authentication, federation support, integrations of IAM into all services, and API support.
- **Monitoring and logging tools:** Deep visibility into API calls, log aggregation tools, alerts, and reduced risks.
- **AWS Marketplace:** Anti-malware, intrusion prevention systems (IPSs), and policy management tools.

AWS SECURITY COMPLIANCE PROGRAMS

How does Amazon measure their success when it comes to compliance with security best practices and regulations? The success of their many customers! Customers drive AWS efforts in these categories (to name just a few):

- Compliance reports
- Attestations
- Certifications

Compliance programs and your adherence to them will actually help you implement excellent security at scale in AWS. This should also help you realize cost savings overall when it comes to your security implementation.

Amazon, especially once you are a customer, will communicate its security responsibilities, success, failures, and overall efforts using the following means:

- Obtaining industry certifications
- Obtaining independent, third-party attestations
- Publishing security information whitepapers and web content
- Providing certificates, reports, and other documents to customers, sometimes under a nondisclosure agreement (NDA)

Amazon also provides the following to customers:

- Functionality through security features
- Compliance playbooks
- Mapping documents

AWS also offers a robust risk and compliance program that helps you with the following:

- Risk management
- Control environments
- Information security



Amazon regularly scans all public-facing points for vulnerabilities. They will even use independent, third-party

firms to perform threat assessments against their technologies and infrastructure. If you (as a customer) are interested in performing penetration (pen) testing against your resources, you may do so, but you must obtain explicit permission from AWS.



Remember, as a customer of AWS, you should (must):

- Engage in a robust security lifecycle approach that includes a review phase, a design phase, and then phases of identification and verification. The identification phase should include external controls that are required to secure the customer resources.
- Understand the required compliance objectives.
- Establish a control environment.
- Understand the validation based on risk tolerances.
- Consistently verify the effectiveness of the security measures deployed.

For more information regarding AWS and security compliance, you can visit the compliance home page for AWS at <https://aws.amazon.com/compliance>. You will discover a wealth of valuable resources linked from this page, which is shown in [Figure 6-3](#).



Figure 6-3 The AWS Security Compliance Home Page

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the

exercises here, Chapter 16, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 6-2 lists these key topics and the page numbers on which each is found.



Table 6-2 Key Topics for Chapter 6

Key Topic Element	Description	Page Number
List	Security tools in AWS	
Overview	Penetration testing	
List	AWS customer security responsibilities	

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

Confidentiality

integrity

availability

compliance

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. Why might you turn to the AWS Marketplace when working on your security infrastructure in AWS?
2. What should you do if you are interested in penetration testing your AWS data and resources?

Chapter 7

AWS Access Management Capabilities

This chapter covers the following subjects:

- **Identity and Access Management:** Where would your AWS architecture be without the ability to secure it? It would be in a very, very bad place. IAM is a key ingredient for AWS security, and this section of the chapter ensures you understand the components of IAM in AWS and how the parts work together to help secure your environment.
- **Best Practices with IAM:** While AWS makes IAM pretty simple, you should always follow the generally accepted best practices. This part of the chapter provides these best practices to you.

You need your users and your fellow engineers to be able to authenticate against AWS and then have their access strictly defined. AWS Identity and Access Management (IAM) is the primary tool for these responsibilities. In this chapter, get ready for a deep dive into IAM.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. [Table 7-1](#) lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 7-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions
Identity and Access Management	1–2
Best Practices with IAM	3–4

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. IAM can permit access to accounts that have already been authenticated in another domain or application. What is this called?

- a.** Proxy trust
 - b.** Role sharing
 - c.** Proxy
 - d.** Federation
- 2.** What identity in IAM is very similar to a user account but has no credentials associated with it?
 - a.** Groups
 - b.** Roles
 - c.** Proxy users
 - d.** Principles
- 3.** Why might you create many different accounts for one of your AWS engineers?
 - a.** To follow the concept of least privilege
 - b.** To reduce the resources required by IAM
 - c.** To provide back doors into the system
 - d.** To ensure you can log activity
- 4.** In a high security environment, what should you do with privileged user accounts?
 - a.** Store credentials in an S3 bucket
 - b.** Create roles that mimic the accounts
 - c.** Use MFA with these accounts
 - d.** Share the access keys with other accounts that require access

FOUNDATION TOPICS

IDENTITY AND ACCESS MANAGEMENT

When it comes to accessing your account (the root account) and then working inside of it, you need the Identity and Access Management (IAM) services of AWS. IAM allows you to grant access to other individuals for team management of the services. IAM permits extremely granular permissions. For example, you might grant someone read access to only a single bucket of objects in S3. Other features of IAM include the following:

- **Access from service to service in AWS:** For example, you can have an application running on an EC2 instance access an S3 bucket. As you will learn later in this chapter, we often use roles for such access.
- **Multi-factor authentication (MFA):** Permitting access through a password and a code from an approved device, thus strengthening security greatly. [Figure 7-1](#) shows the configuration area for MFA in the IAM Management Console.

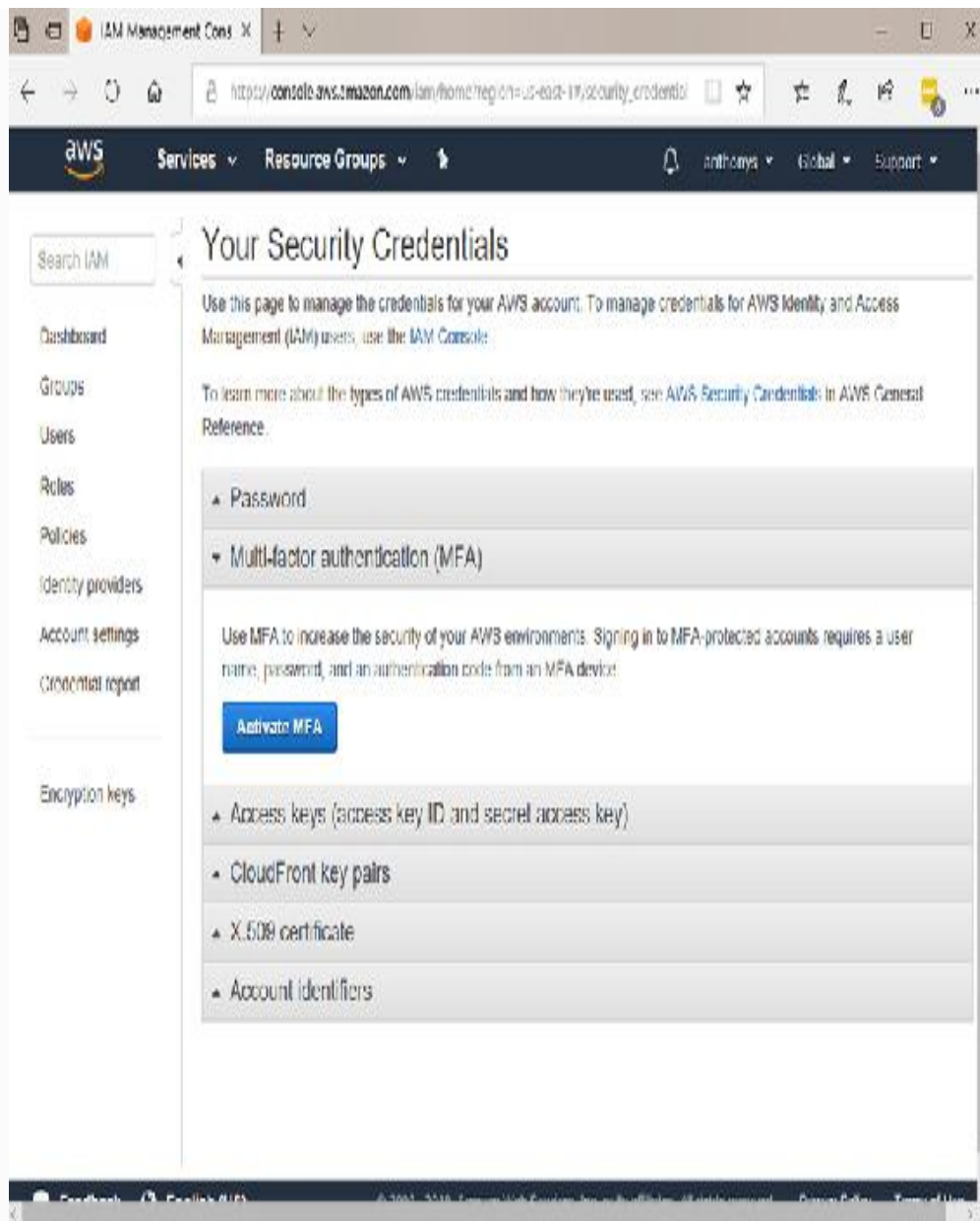


Figure 7-1 Configuring MFA for an Account

- **Identity federation:** Users who have already authenticated with another service can gain temporary access to resources and services in your account.
- **Identity information for assurance:** CloudTrail can trace and log all SPI activity against every service and resource

in your account. Figure 7-2 shows the CloudTrail Dashboard in AWS.

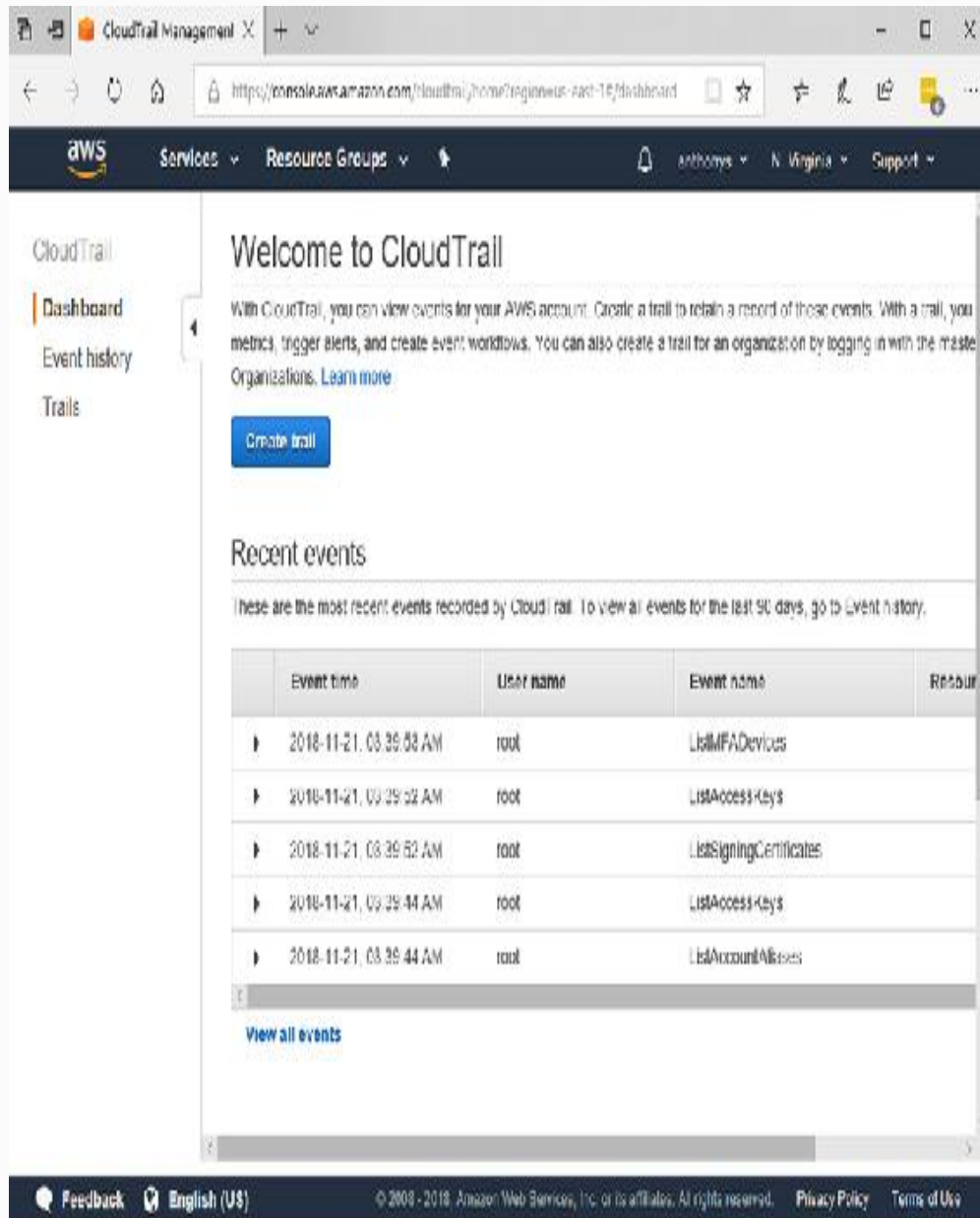


Figure 7-2 The CloudTrail Dashboard

- **PCI DSS compliance:** IAM supports the processing, storage, and transmission of credit card data by a merchant

or service provider, and it has been validated as being compliant with the Payment Card Industry (PCI) Data Security Standard (DSS).

- **Integration:** In order to be successful, IAM integrates with every major service of AWS.
- **Eventually consistent:** Amazon replicates important data around the world with their Global Infrastructure, to help ensure high availability (HA). As a result, data in some locations might lag others. Therefore, with IAM, consider implementing your changes for IAM first, then verify full replication before working with dependent service deployments.
- **Always free:** While some services of AWS can be used for one year free (using the Free Tier account), IAM services remain free for the life of your account.
- **Accessibility options:** You can access the components of IAM in a variety of ways, including the AWS Management Console, AWS command-line tools, AWS SDKs, and the IAM HTTPS API.



It is critical that you understand the main identities you'll use in IAM. Please realize that there is much more to IAM than these identities, but at this point in your AWS education, we are covering the main foundational components.

Identities consist of the following:

- **AWS account root user:** This is the account you established when you signed up for AWS; note that the user name for this account is the email address used for signup.
- **Users:** These are the entities you create in AWS to represent the people or services that use the IAM user to interact with AWS. When you create an IAM user, you grant it permissions by making it a member of a group that has appropriate permission policies attached (recommended) or by directly attaching policies to the user. You can also clone the permissions of an existing IAM user, which automatically makes the new user a member of the same groups and attaches all the same policies. Figure 7-3 shows a user in AWS.

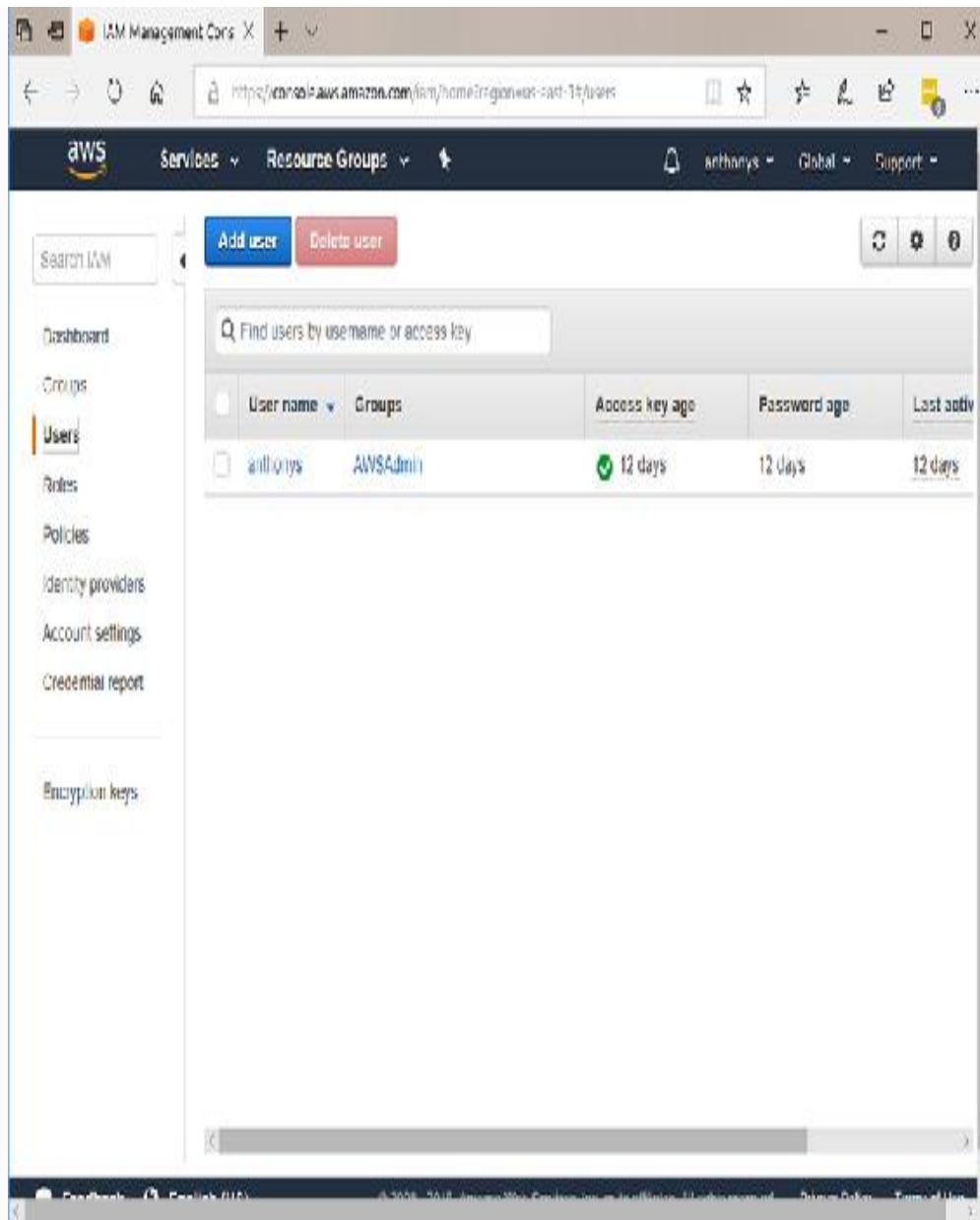


Figure 7-3 A User in AWS IAM

- **Groups:** A collection of IAM users. You can use groups to specify permissions for a collection of users, which can make those permissions easier to manage for those users.
- **Roles:** These are similar to user accounts, but they do not have any credentials (password or access keys) associated

with them.

BEST PRACTICES WITH IAM

While IAM in AWS provides many exciting capabilities, its complexity can cause organizations to make fatal flaws when working with the service. This is why following best practices is critical.



You should consider following most (if not all) of these recommendations.

- **Store root user access keys securely:** The root user account for your AWS implementation should be used infrequently. With this said, it is critical that you protect the access key ID and secret access key for this account. You must ensure that you have these credentials protected in your own infrastructure and treat them with the upmost care. In fact, in high security environments, consider not defining access keys for the root account. Instead, use the email address, a complex password, and physical multi-factor authentication instead for the rare times this account must be used.
- **Create individual IAM users:** Because you do not want to use the root account for your AWS implementation, it is critical that you create additional user accounts. This would include for yourself so that you are not required to use the root account. In larger organizations, you will have

a large team working on AWS. You must create multiple accounts for your staff to ensure that everyone is authenticating and being authorized for only those resources and permissions that are required for each member to do their jobs. You will most likely have at least one account in IAM for every person who requires administrative access.

- **Use groups to assign permissions to IAM users:** Even though it might seem silly, if you are the sole administrator of your AWS implementation, you will want to create a group and assign permissions to this group. Why? If you do need to grow and hire another administrator, you can just add that user account to the group you created. We always want our AWS implementations to scale, and using groups helps ensure this. It should also be noted that applying permissions to groups instead of individual user accounts will also help eliminate assignment errors, as we are minimizing the amount of permissions we must grant.
- **Use AWS-defined policies for permissions:** Amazon was very kind to us. They defined a ton of policies we can easily leverage when working with IAM. What's more, AWS maintains and updates these policies as they introduce new services and API operations. The policies that AWS created for us are defined around the most common tasks we need to perform. These make up an excellent starting place for your own policies. You can copy a given policy and customize it to make it even more secure. Oftentimes, you will find the default defined policies are too broad with access.

- **Grant least privilege:** Why might you end up with many different accounts for yourself in AWS? Well, you always want to sign in with the account that provides the least amount of privileges for what you are trying to accomplish. That way, if an attacker does manage to capture your security credentials and begins acting as you in the AWS architecture, they can do a limited amount of damage. For example, if you need to simply monitor the files in AWS S3 buckets, you can use an account with only read permissions on these buckets. This would certainly limit the damage an attacker can carry out.
- **Review IAM permissions:** You should not use a “set and forget” policy when it comes to your permissions in IAM. You should consistently review the permissions level assigned to ensure that you are following least privilege concepts and that you are still granting those permissions to the groups that require them. There is even a policy summary option within IAM to facilitate this.
- **Always configure a strong password policy for your users:** It is a sad fact of human nature. Your users will tend to be lazy about setting (and changing) their passwords. They will tend to use simple passwords that are easy for them to remember. Unfortunately, these simple passwords are also easy to crack. Help your security by setting a strong password policy that your users must adhere to. Figure 7-4 shows the configuration of a password policy for user accounts in the IAM Management Console.

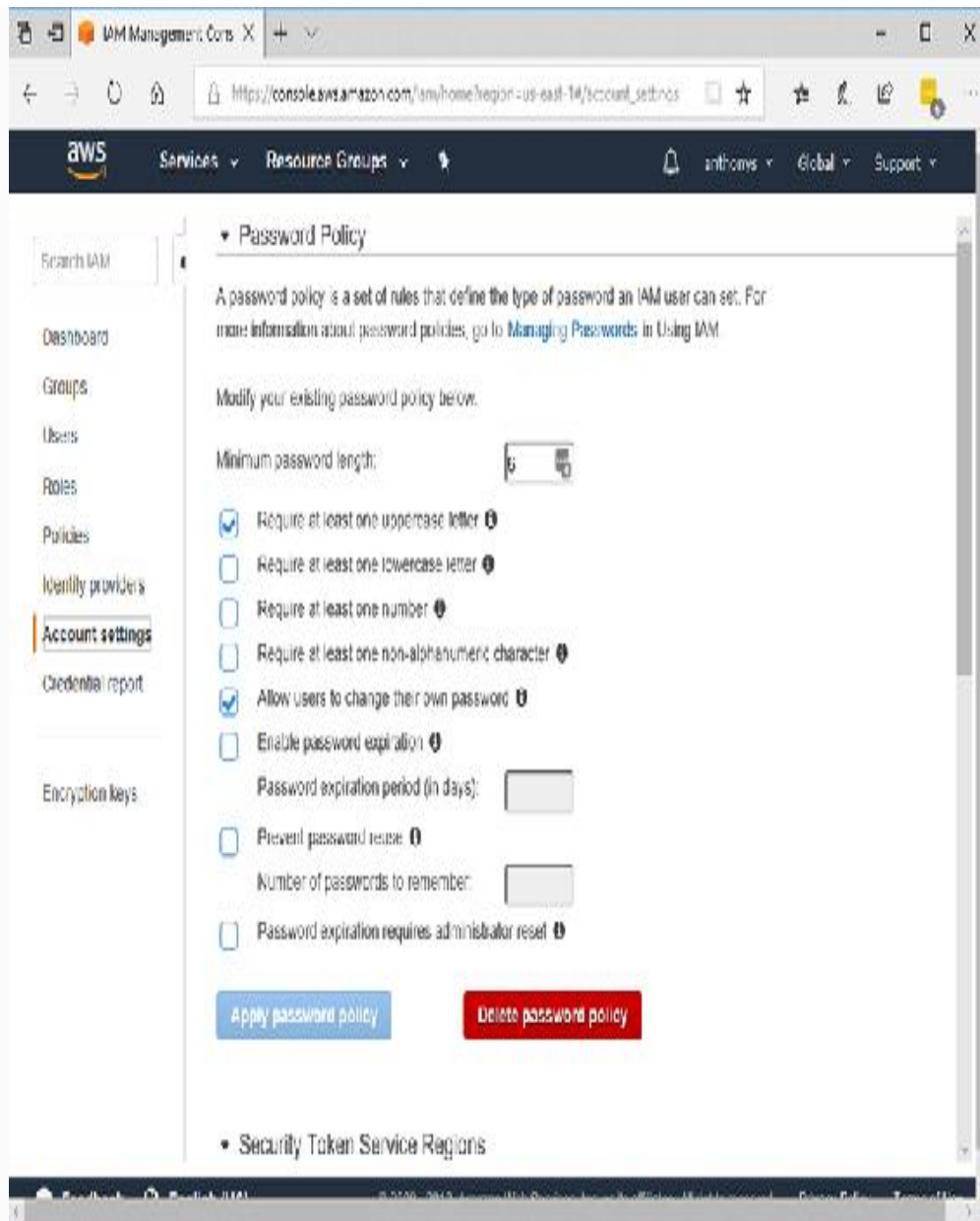


Figure 7-4 Configuring a Password Policy

- **Enable multi-factor authentication for privileged user accounts:** Of course, you do this for the seldom-used AWS root account, but you should also protect key admin accounts you have created in AWS. Using multi-factor authentication (MFA) ensures the user knows something

(like a password) and also possesses something (like a smartphone). With most AWS environments today, MFA is considered mandatory.

- **Use roles:** You should consider the use of roles in AWS when you have applications or services running on EC2 instances that need to access other services or resources.
- **Use roles to delegate permissions:** Roles can also prove very valuable when you need to permit one AWS account to access resources in another AWS account. This is a much more secure option to providing the other AWS account with username and password information for your account.
- **Do not share access keys:** It might be tempting to take the access keys that permit programmatic access to a service or resource and just share those with another account that needs the same access. Resist this temptation. Remember, you can always create a role that encompasses the required access.
- **Rotate credentials:** Be sure to change passwords and access keys regularly in AWS. The reason for this, of course, is the fact that if these credentials are compromised, you will have minimized the damage that can be done when the stolen credentials no longer function!
- **Remove unnecessary credentials:** Because it is so easy to learn and test new features in AWS, it can get messy as far as IAM components you leave in place that are no longer needed. Be sure to routinely audit your resources for any

“droppings” that are no longer needed. AWS even assists in this regard with structuring reports around credentials that have not been recently used.

- **Use policy conditions:** Always consider building conditions into your security policies. For example, access might have to come from a select range of IP addresses. Or MFA might be required. Or there can be time-of-day or day-of-week conditions.
- **Monitor, monitor, monitor:** AWS services provide the option for an intense amount of logging. Here are just some of the services where careful logging and analysis can dramatically improve security:
 - CloudFront
 - CloudTrail
 - CloudWatch
 - AWS Config
 - S3

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the exercises here, [Chapter 16, “Final Preparation,”](#) and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 7-2 lists these key topics and the page numbers on which each is found.



Table 7-2 Key Topics for Chapter 7

Key Topic Element	Description	Page Number
List	Identities in IAM	
List	Best practices with IAM	

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

IAM

MFA

federation

users

groups

roles

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. What is often used when you need to provide access from an application running on an EC2 instance to other resources within AWS?
2. What account is created when you sign up for AWS, but then should be used very sparingly after that point?

Chapter 8

Resources for Security Support

This chapter covers the following subjects:

- **Tools for Security Support:** This section of the chapter details various important tools for security support in AWS.
- **Additional Security Support Resources:** This section of the chapter provides even more security support resource ideas that are available to you as an AWS customer, or even as a potential customer.

Greater security than ever before in your infrastructure and architectures is possible within AWS. In order to achieve the highest levels of security and the lowest levels of risk, you should be ready to take advantage of the tremendous resources available to you for security support. This chapter is critical in this regard.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. Table 8-1 lists the major headings in this chapter and the “Do I Know This Already?”

quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 8-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions
Tools for Security Support	1-2
Additional Security Support Resources	3-4

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1.** What is a central resource for compliance-related AWS information?
 - a.** CodeLearn
 - b.** Lambda
 - c.** Artifact
 - d.** ProtectGuard

2. What acts like your own cloud expert in AWS, providing recommendations for greater security based on your existing configurations?
- a. Trusted Advisor
 - b. Artifact
 - c. EC2
 - d. Cognito
3. What Learning Path is recommended for those in compliance roles in your AWS architecture?
- a. Code Learning Path
 - b. SysOps Learning Path
 - c. Architect Learning Path
 - d. Auditor Learning Path
4. From where does Amazon often draw information for certification exam questions?
- a. Case studies
 - b. Security blogs
 - c. Security bulletins
 - d. FAQs

FOUNDATION TOPICS

TOOLS FOR SECURITY SUPPORT

When you have a topic as critical as security, you need a wealth of tools to assist you. With AWS, that is exactly what you get.

Certifications and Attestations



The number of certifications and attestations for AWS regarding security is pretty staggering. And to think this list is constantly growing! These certifications and attestations help you ensure that you are meeting the levels of security that you might be required to provide.

Assurance programs in this category include the following:

- DoD SRG
- FedRAMP
- FIPS
- IRAP
- ISO 9001
- ISO 27001
- ISO 27017
- ISO 27018
- MLPS Level 3
- MTCS
- PCI DSS Level 1

- SEC Rule 17a-4(f)
- SOC 1
- SOC 2
- SOC 3

There are many laws and regulations you might need to meet. Fortunately, AWS allows for the following requirements:

- EU Model Clauses
- FERPA
- HIPAA
- IRS-1075
- ITAR
- My Number Act (Japan)
- VPAT / Section 508
- EU Data Protection Directive

Finally, AWS adheres to many frameworks recommended for security, including the following:

- CJIS
- FedRAMP TIC
- FISC
- FISMA
- GxP (FDA 21 CFR Part 11)
- IT-Grundschutz

- MPAA
- NERC
- NIST
- UK Cyber Essentials

Whitepapers

It is almost a bit of a cliché these days—turning to whitepapers for assistance is that commonplace. We must admit, however, that it is a very important step in security. AWS understands this, and provides many important whitepapers related directly to security.

Want to get excited over just some of these titles? Check out Table 8-2!

Table 8-2 AWS Security Related Whitepapers

Whitepaper	Date of Publication
AWS Well-Architected Framework – Security Pillar	July 2018
Architecting for Genomic Data Security and Compliance in AWS	December 2014
AWS Key Management Service Best Practices	April 2017
AWS Risk & Compliance	May 2017
AWS Risk and Compliance Overview	January 2017
AWS Governance at Scale	July 2018
AWS Security Best Practices	August 2016
Overview of AWS Security – Application Services	June 2016
Introduction to Auditing the Use of AWS	October 2015
AWS: Overview of Security Processes	May 2017
CSA Consensus Assessments Initiative Questionnaire	May 2017
AWS Certifications, Programs, Reports, and Third-Party Attestations	March 2017
Automating Governance on AWS	August 2015
AWS Answers to Key Compliance Questions	January 2017
AWS Best Practices for DDoS Resiliency	June 2018
Introduction to AWS Security	July 2015
Overview of AWS Security – Analytics, Mobile, and Application Services	June 2016

AWS Artifact

AWS Artifact is your go-to, central resource for compliance-related information that matters to you. It provides on-demand access to AWS's security and compliance reports and select online agreements. Reports available in AWS Artifact include Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls. Agreements available in AWS Artifact include the Business Associate Addendum (BAA) and the Nondisclosure Agreement (NDA).

AWS Trusted Advisor

Wouldn't it be nice if we had our own cloud expert working for us at AWS? This is the concept behind the Trusted Advisor tool. This management tool ensures you are following security best practices and helps you close security gaps.

LAB: Using the Trusted Advisor



This lab walks you through the steps of using the Trusted Advisor to learn of security issues and improvements you might be able to make to enhance your AWS security.

Note

This lab assumes you have an AWS account. If you do not, this book has a lab in Chapter 12, "AWS Cloud Economics," that helps you create an account using the free tier of AWS.

Follow these steps in order to use Trusted Advisor:

Step 1. In the AWS Management Console, search for **Trusted Advisor**. Select the **Trusted Advisor** link that appears.

Step 2. In the dashboard on the left side of the page, click **Security**.

Step 3. Note the security checks that have been performed and the results. Notice also the other security checks that may be purchased. Figure 8-1 shows the security checks.

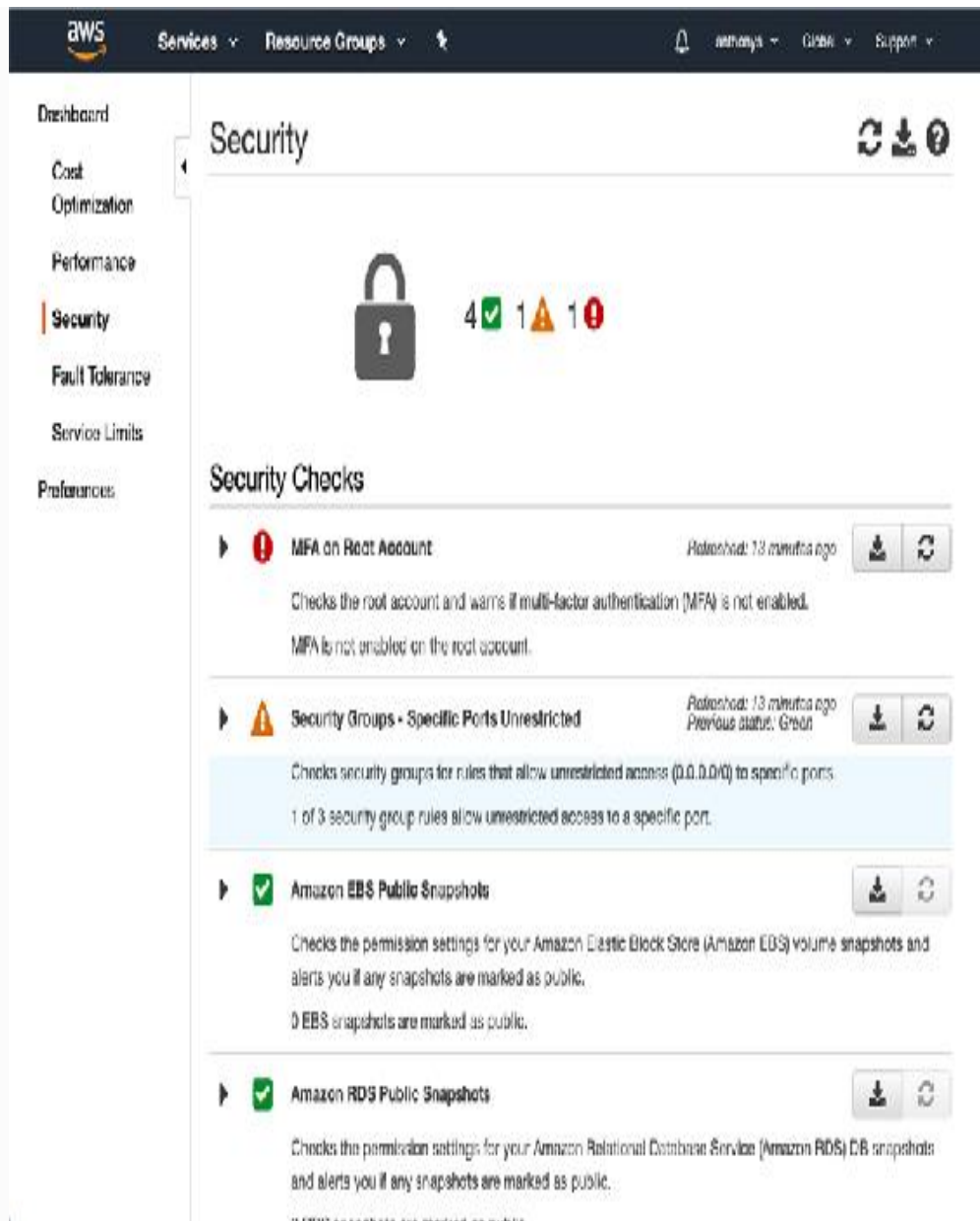


Figure 8-1 Using the Trusted Advisor for Security Guidance

AWS Cloud Support Associates and Engineers

Oftentimes, your first point of contact when it comes to security issues and problems will be the support staff of AWS.

These employees are called *Cloud Support Associates* and also *Cloud Support Engineers*.

Remember, there are different levels of support you can purchase from AWS. [Table 8-3](#) shows the support levels and the support options included.

Table 8-3 Technical Support Options with AWS

Basic	Developer	Business	Enterprise
None	Business hours access to Cloud Support Associates via email	24×7 access to Cloud Support Engineers via email, chat, and phone	24×7 access to Senior Cloud Support Engineers via email, chat, and phone

ADDITIONAL SECURITY SUPPORT RESOURCES

Believe it or not, there are even more security support resources than we have mentioned thus far in the chapter. This section explores even more of them.

Professional Services Network

The [AWS Professional Services](#) organization is a global team of experts that can help you realize your desired business outcomes when using the AWS Cloud. Amazon works together with your team and your chosen member of the [AWS Partner Network \(APN\)](#) to execute your enterprise cloud computing initiatives.

The AWS Professional Services organization provides assistance through a collection of offerings that help you achieve specific outcomes related to enterprise cloud adoption. AWS Professional Services also deliver focused guidance through their global specialty practices, which cover a variety of solutions, technologies, and industries. In addition to working alongside AWS customers, AWS Professional Services share their experience through tech talk webinars, whitepapers, and blog posts that are available to anyone.

AWS Partner Network

The AWS Partner Network (APN) is the global partner program for AWS. It is focused on helping APN Partners build successful AWS-based businesses or solutions by providing business, technical, marketing, and go-to-market support.

APN Partners receive business, technical, sales, and marketing resources to help you to grow your business and better support your customers. You can join the APN and take advantage of numerous APN programs to differentiate your business and connect with customers on AWS.

The AWS Partner Network strives to ensure customers take full advantage of all the business benefits that AWS has to offer. With their deep expertise in AWS, APN Partners are uniquely positioned to help your company at any stage of your cloud adoption journey and to help you achieve your business objectives.

Advisories and Bulletins

No matter how carefully engineered the AWS services are, from time to time it may be necessary to notify customers of security and privacy events with AWS services. As a result, Amazon publishes security bulletins that are publicly accessible via their website. You can also subscribe to the Security Bulletin RSS Feed to keep abreast of security announcements.

Here is a sample AWS Security bulletin:

TITLE: L1 Terminal Fault Speculative Execution Issue

DATE: August 16, 2018 2:45 PM PDT

CVE IDENTIFIERS: CVE-2018-3620, CVE-2018-3646

CONTENTS: Intel has published a security advisory (INTEL-SA-00161) regarding a new side-channel analysis method concerning their processors called “L1 Terminal Fault” (L1TF). AWS has designed and implemented its infrastructure with protections against these types of attacks, and has also deployed additional protections for L1TF. All EC2 host infrastructure has been updated with these new protections, and no customer action is required at the infrastructure level. Updated kernels for Amazon Linux AMI 2017.09 (ALAS-2018-1058), Amazon Linux AMI 2018.03 (ALAS-2018-1058), and Amazon Linux 2 (ALAS-2018-1058) are available in the respective repositories. As a general security best practice, we recommend that customers patch their operating systems or software as relevant patches become available to address emerging side-channel issues. We have released new versions of the Amazon Linux and Amazon Linux 2 AMIs that

automatically include the updated kernel. AMI IDs for images with the updated kernels can be found at Amazon Linux 2018.03 AMI IDs, Amazon Linux 2 AMI IDs, and in the AWS Systems Manager Parameter Store. Meanwhile, we suggest using the stronger security and isolation properties of EC2 instances rather than relying on operating system process boundaries or containers when workloads execute with different security privileges.

Auditor Learning Path

The [AWS Auditor Learning Path](#) is designed for those in auditor, compliance, and legal roles who want to learn how their internal operations can demonstrate compliance using AWS's platform. Thanks to this Learning Path, you can build the skills necessary to understand how to audit solutions on the AWS Cloud.

Compliance Solution Guide

The AWS Compliance Solution Guide is designed to provide you with a repository of frequently used resources and processes needed to perform your compliance responsibilities on AWS.

AWS protects millions of active customers around the world—from large enterprises and government organizations, to startups and nonprofits. Through these relationships, Amazon has developed best-in-class resources to allow customers from any industry to quickly understand how to achieve compliance in the AWS Cloud. Customers inherit all of the benefits of the

vast experience of the AWS staff, including best practices for security policies, architecture, and operational processes validated against external assurance frameworks.

Services in Scope

AWS also includes services in the scope of their compliance efforts based on the expected use case, feedback and demand. If a service is not currently listed as in scope of the most recent assessment, it does not mean that you cannot use the service. It is part of the shared responsibility for your organization to determine the nature of the data. Based on the nature of what you are building on AWS, you should determine if the service will process or store customer data and how it will or will not impact the compliance of your customer data environment.

Amazon encourages you to discuss your workload objectives and goals with your AWS account team; they will be able to evaluate your proposed use case and architecture, and how the AWS security and compliance processes overlay that architecture.

Security Blog

Amazon also provides a security-centric blog site that is continuously updated with the latest important announcements and training opportunities on security-related developments.

Figure 8-2 shows the AWS Security Blog.

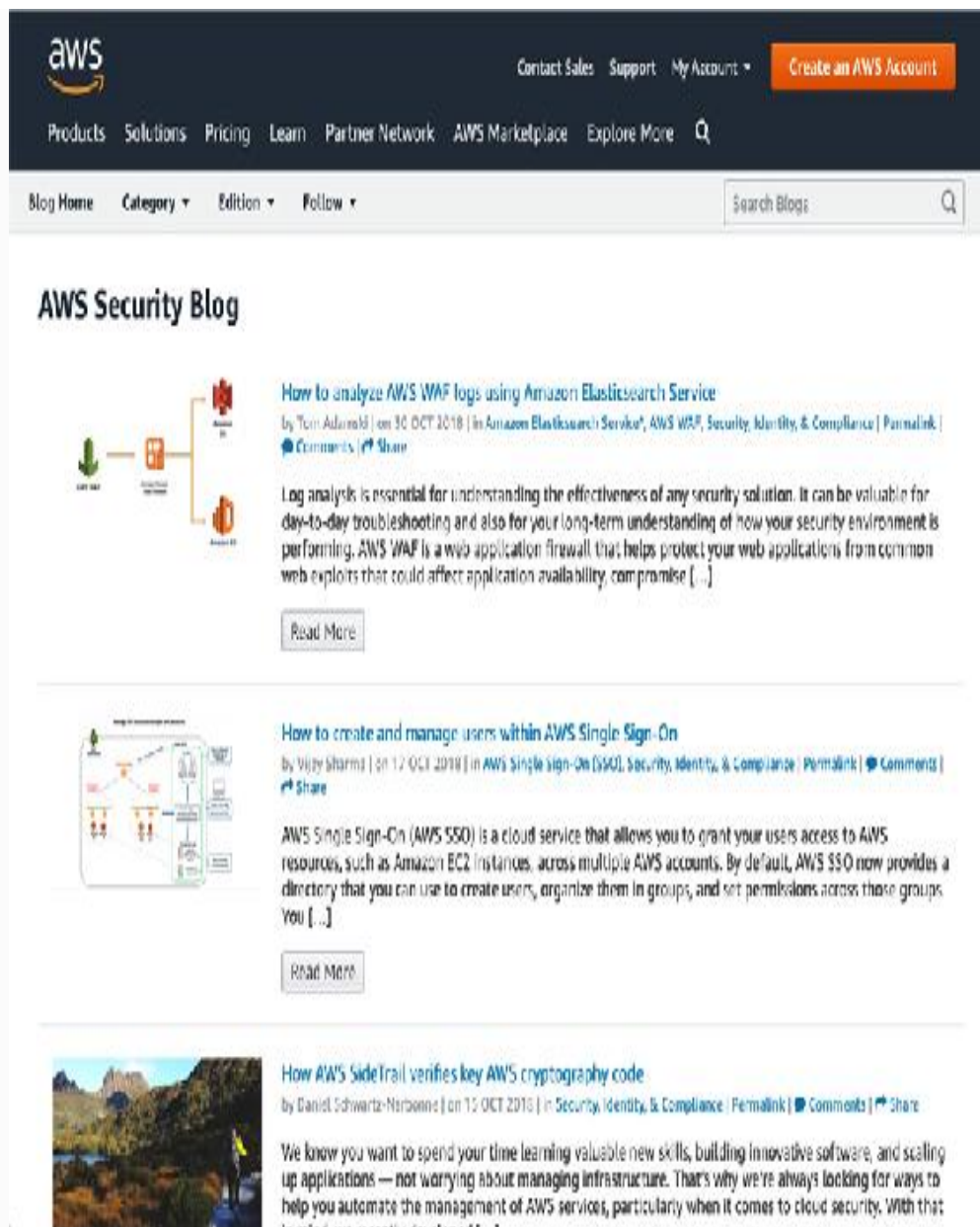


Figure 8-2 The AWS Security Blog

Case Studies

Amazon also does an excellent job of maintaining case studies for you to learn security best practices through. These case

studies are available online, and they can even be selected based on topic.

FAQs



Another excellent resource is the Frequently Asked Questions (FAQs) area of the AWS documentation. Here, you can visit those FAQs regarding security. These present an excellent learning opportunity. These FAQs are also a valuable certification exam prep resources, as Amazon admits that they love to derive exam questions from these very robust and detailed FAQs.

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the exercises here, [Chapter 16, “Final Preparation,”](#) and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. [Table 8-4](#) lists these key topics and the page numbers on which each is found.



Table 8-4 Key Topics for Chapter 8

Key Topic Element	Description	Page Number
Overview	Certifications and attestations	
Lab	Using the AWS Trusted Advisor	
Overview	FAQs	

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

Whitepapers

AWS Artifact

Trusted Advisor

AWS Professional Services

AWS Partner Network

AWS Auditor Learning Path

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. Provide at least three examples of security frameworks to which AWS adheres.
2. What level of technical support provides 24×7 access to Senior Cloud Support Engineers via email, chat, and phone?

Part III

Domain 3: Technology

Chapter 9

Methods of Deploying and Operating in AWS

This chapter covers the following subjects:

- **Automation**: Automation is a key driver with the adoption of cloud technologies. This section of the chapter discusses many of the technologies of AWS and the approaches taken to automation.
- **Orchestration**: Orchestration takes automation even further, permitting the coordination and scheduling of many different automation events. This part of the chapter walks you through some of the orchestration that is possible with AWS.
- **Management Options**: There are many ways to manage AWS effectively. This section of the chapter lays each one out for you in detail.

This chapter focuses on getting things done in AWS in the most efficient and cost-effective manner. Using automation and orchestration can also dramatically improve performance and security due to the reduction errors in configurations and the elevation of configuration consistency. This chapter also

ensures you know details about the many, many methods you can use to manage AWS.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. [Table 9-1](#) lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 9-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions
Automation	1-2
Orchestration	3-4
Management Options	5-6

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly

guess skews your self-assessment results and might provide you with a false sense of security.

1. Why is automation so easily accommodated in AWS?

- a.** Because CloudTrail provides automation templates automatically for you
- b.** Because multiple regions facilitate code deployment
- c.** Because physical systems host the EC2 instances you work with daily
- d.** Because all actions can be implemented through API calls

2. Which of the following is not considered a benefit of automation?

- a.** Reduction in required security measures
- b.** Lowered operating costs
- c.** Simpler and faster code deployment
- d.** Reduction in the potential for errors

3. What is the result of orchestration?

- a.** An architecture guaranteed to be free of errors
- b.** Alignment of all required tasks in an independent execution environment
- c.** A consolidated process or workflow
- d.** An environment that can be replicated easily on any public cloud platform

4. Which is not considered a benefit of orchestration?

- a. The lowering of overall IT costs
 - b. The elimination of the need for experimentation
 - c. Improved delivery times
 - d. Reduced friction between different teams
5. CloudWatch falls into which category of management options?
- a. Provisioning
 - b. Managed Services for Configuration
 - c. Operations Management
 - d. Monitoring and Logging
6. What is the fully managed configuration management service in AWS?
- a. CloudTrail
 - b. OpsWorks
 - c. CloudFormation
 - d. CloudWatch

FOUNDATION TOPICS

AUTOMATION

Automation is one of the reasons so many technical engineers are driven to a love of cloud technologies. In the case of AWS, there is a huge emphasis on API calls in order to configure the

architecture. This permits automation of everything associated with AWS.



Automation incorporates elements such as the following:

- Configuration templates
- Code deployment automation
- Self-healing infrastructures
- Reduction in the need for manual interventions
- Reduction in the potential for errors
- Lowered operating costs for Managed Service Providers (MSPs)

For many organizations relying on AWS nowadays, approaching any challenge for their IT organization begins with the question, “How can we automate the solution?” Perhaps it is the corporate policy in your organization that you cannot use any of the default resources created for you in AWS. Sure, you could go in to the Management Console and do lots of potentially error-prone mouse clicking, but things are so much easier (and more accurate) when you can automate such actions with a script.



What are some common areas where automation tends to play a huge role in AWS? Here are just a few:

- Backup generation and retention
- Security compliance
- Code deployments
- AWS infrastructure changes

Remember, because AWS takes an API-centric approach, there is really nothing you cannot automate. The short list given here is just areas where automation is frequently in use by AWS customers.

ORCHESTRATION

A huge point of confusion for many engineers new to AWS and cloud technology is understanding the differences between cloud automation and cloud orchestration. One of the reasons why stems from the fact that the two terms are often used interchangeably, which is often incorrect. The differences between these concepts highlight a key challenge for teams looking to improve IT processes.

Let's begin by reviewing automation. *Automation* describes a task or function accomplished without human intervention. So then what is orchestration? *Orchestration* describes the arranging and coordination of automated tasks, ultimately resulting in a consolidated process or workflow. Automation and orchestration go hand-in-hand, but note that they are technically different concepts.

With AWS, we like to (and are encouraged to) create standard processes to spin up full environments to host new and exciting applications. We accomplish this by orchestrating many automated tasks. These might include the following:

- Automating new instances with Auto Scaling.
- Load balancing with automated ELB configurations.
- Deploying automation using a tool like CodeDeploy in AWS. Figure 9-1 shows the Getting Started page of CodeDeploy in the AWS Management Console.
- Using Puppet scripts to automate the configuration of the OS.



Figure 9-1 CodeDeploy in AWS

While individually the tasks in the preceding list might be fairly simple to automate with the robust tools and capabilities of AWS, taken together these tasks can be very tricky to orchestrate. After all, these activities must occur in a particular order, under certain security groups/tools, and be given roles and granted permissions. In other words, engineers must complete hundreds of manual tasks to deliver the new

environment, even when the building blocks of that environment are automated. This is where orchestration is key.

Cloud orchestration tools, whether native to the IaaS (Infrastructure as a Service) platform or third-party software tools, enumerate the resources, instance types, IAM roles, and other resources required. Orchestration can also enumerate the configuration of these resources and the interconnections between them.

AWS engineers can use tools like CloudFormation to create declarative templates that orchestrate these processes into a single workflow so that the “new environment” workflow previously described becomes a single API call.

Well-orchestrated IT processes enable and empower continuous integration and continuous delivery, uniting teams in the creation of a set of templates that meet developer requirements. Such templates are in many ways living documents that embody the celebrated and popular DevOps philosophy.



The benefits of orchestration tools far outweigh any potential drawbacks. For organizations today, they celebrate such advantages as the following:

- The lowering of overall IT costs
- Gained time for new or experimental projects

- Improved delivery times to customers
- Reduced friction between system and development teams

MANAGEMENT OPTIONS

There is an incredibly impressive range of options when it comes to managing AWS. These tools fall into the following subcategories:

- **Provisioning:** CloudFormation is the primary management service in this category. It provides a common language for you to describe and provision all the infrastructure resources in your cloud environment. CloudFormation allows you to use a simple text file to model and provision all the resources needed for your applications across all regions and accounts. What's more is the fact that it can accomplish this in an automated and secure manner. Once everything is modeled in CloudFormation, this text file serves as the single "source of truth" regarding the resources of your cloud environment. It is recommended that you also create a collection of approved CloudFormation files in an AWS Service Catalog to allow your organization to only deploy approved and compliant resources.
- **Operations Management:** AWS provides a set of services for systems and operations management that allows you to control your infrastructure resources with proper governance and compliance. You can use AWS Systems Manager to quickly view and monitor all your resources

and automate common operational tasks, such as patching and state management. Systems Manager provides a unified user interface, enabling you to easily manage your cloud operations activities in one place. You can also use CloudTrail for logging user activities within your organization and AWS Config for inventorying all configurations across your resources. Figure 9-2 shows CloudTrail in AWS.

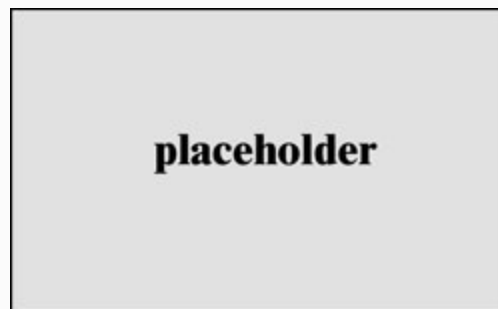


Figure 9-2 CloudTrail in AWS

- **Monitoring and Logging:** CloudWatch is the primary monitoring service for AWS cloud resources and the applications you run on AWS. You can use CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources. CloudWatch can monitor AWS resources such as EC2 instances, DynamoDB tables, and RDS DB instances, as well as any custom metrics or log files generated by your applications. CloudWatch also provides a stream of events describing changes to your AWS resources that you can use to react to changes in your applications.

- **Managed Services for Configuration:** The main tool in this area is AWS OpsWorks. OpsWorks is a fully managed configuration management service that hosts and scales Chef Automate and Puppet Enterprise servers. OpsWorks eliminates the need to install and operate your own configuration management systems or worry about scaling its infrastructure. It also works seamlessly with your existing Chef and Puppet tools. OpsWorks will automatically patch, update, and back up your Chef and Puppet servers as well as maintain the availability of them. OpsWorks is an excellent choice if you are an existing user of Chef or Puppet.



Remember, to access your AWS resources from a management perspective, you also have many options. Here are just some of these options:

- The AWS Management Console.
- The AWS CLI. Figure 9-3 shows the AW CLI installed on my local Windows machine being accessed from my local command prompt.
- Programmatic access using SDKs and APIs.

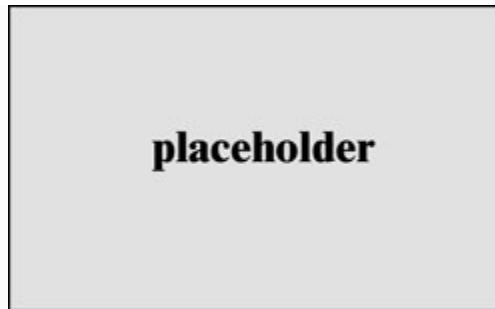


Figure 9-3 The AWS CLI

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the exercises here, [Chapter 16, “Final Preparation,”](#) and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. [Table 9-2](#) lists these key topics and the page numbers on which each is found.



Table 9-2 Key Topics for [Chapter 9](#)

Key Topic Element	Description	Page Number
List	Automation elements	
List	Common areas using automation	
List	Benefits of orchestration	
List	Management access options in AWS	

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

Automation

orchestration

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. Name at least two areas where automation is often used in AWS.
2. Name at least two management access options for AWS.

Chapter 10

The AWS Global Infrastructure

This chapter covers the following subjects:

- **Regions**: This section describes the concept of regions and what they contain. Although regions are constantly being added, this section gives you a look at the current regions as of this writing and the naming conventions used for them.
- **Availability Zones**: This section provides valuable information about the Availability Zones that exist within regions.
- **Connections**: This section provides details on connection technologies for your AWS global infrastructure interactions.

A key advantage that Amazon provides through AWS is a high-tech, high-speed global infrastructure of advanced data centers around the globe. This chapter describes how the AWS global infrastructure is organized and how you can connect to the infrastructure.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. [Table 10-1](#) lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 10-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions
Regions	1-3
Availability Zones	4-6
Connections	7-9

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. How many Availability Zones (AZs) are located in regions in the AWS Global Infrastructure?
 - a. At least two
 - b. One

- c. Two**
 - d. Three**
- 2.** What is an Edge Location used for in an AWS region?
 - a. CloudFormation**
 - b. RDS**
 - c. S3**
 - d. CloudFront**
- 3.** Which statement regarding regions in AWS is not correct?
 - a. Regions in North America rely on the presence of the other North American regions.**
 - b. Regions are connected with fast connections to other regions.**
 - c. Edge Locations exist inside of regions.**
 - d. Availability Zones exist inside of regions.**
- 4.** How many discrete data centers are located in an AZ in the AWS Global Infrastructure?
 - a. At least one**
 - b. At least two**
 - c. At least three**
 - d. At least four**
- 5.** How does Amazon design each AZ in the AWS Global Infrastructure?

- a.** To be located in the largest city in a region
 - b.** To exist outside of a region
 - c.** As an independent failure domain
 - d.** As dependent on at least one other AZ
- 6.** How is a typical AZ given power in the AWS Global Infrastructure?
 - a.** Via different grids from independent utilities
 - b.** From generators powered by Amazon
 - c.** From a single grid from the highest performance utility
 - d.** From a shared public power station
- 7.** What component allows you to connect privately from your Virtual Private Cloud (VPC) to services you need?
 - a.** VPC endpoint
 - b.** Direct Connect
 - c.** VPN
 - d.** CloudFront
- 8.** What would you use if you have multiple VPCs in AWS and you need to communicate between them?
 - a.** Gateway endpoint
 - b.** VPC peering
 - c.** Direct Connect
 - d.** ClassicLink

9. What technology permits you to use a private connection from your facility to AWS?
- a. ClassicLink
 - b. Direct Connect
 - c. VPC peering
 - d. VPC endpoint

FOUNDATION TOPICS

REGIONS

AWS serves over a million active customers in more than 190 countries. Amazon is steadily expanding their global infrastructure to help customers achieve lower latency and higher throughput and to ensure that their data resides only in the region they specify.



Amazon builds the AWS Cloud infrastructure around regions and Availability Zones (AZs):

- A region is a physical location in the world where there are multiple AZs. Note that a region, by design, must have at least two or more AZs, never just one.
- At the time of this writing, there are 18 regions around the world and 55 AZs. Note that these numbers are now increasing at a faster rate than ever.

Figure 10-1 shows a sample structure of the AWS Global Infrastructure of Regions and Availability Zones.

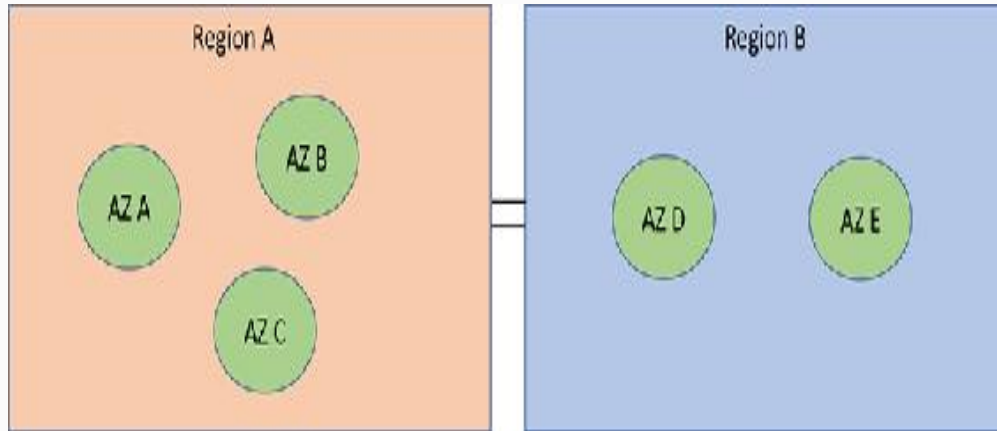


Figure 10-1 The AWS Global Infrastructure

Each Amazon region is designed to be completely isolated from the other Amazon regions. This isolation achieves the highest possible fault tolerance and stability. While each AZ is isolated from a fault tolerance perspective, Amazon connects the AZs within a region through low-latency links.

To give you a sense for regions in AWS, examine the details for some of the North American regions:

- US East (Northern Virginia) Region – EC2 Availability Zones: 6 – Launched 2006
- US East (Ohio) Region – EC2 Availability Zones: 3 – Launched 2016
- US West (Oregon) Region – EC2 Availability Zones: 3 – Launched 2011

- US West (Northern California) Region – EC2 Availability Zones: 3 – Launched 2009
- AWS GovCloud (US-West) Region – EC2 Availability Zones: 3 – Launched 2011
- Canada (Central) – EC2 Availability Zones: 2 – Launched 2016

When you reference regions in your AWS code, you use standardized names created by Amazon for each region. [Table 10-2](#) lists some regions and their official AWS names.

Table 10-2 Regions and Their Names in AWS

Region	Name
US West (Oregon) Region	us-west-2
US West (N. California) Region	us-west-1
US East (Ohio) Region	us-east-2
US East (N. Virginia) Region	us-east-1
Asia Pacific (Mumbai) Region	ap-south-1
Asia Pacific (Seoul) Region	ap-northeast-2
Asia Pacific (Singapore) Region	ap-southeast-1
Asia Pacific (Sydney) Region	ap-southeast-2
Asia Pacific (Tokyo) Region	ap-northeast-1
Canada (Central) Region	ca-central-1
China (Beijing) Region	cn-north-1
EU (Frankfurt) Region	eu-central-1
EU (Ireland) Region	eu-west-1
EU (London) Region	eu-west-2
EU (Paris) Region	eu-west-3
South America (São Paulo) Region	sa-east-1
AWS GovCloud (US)	us-gov-west-1

The AWS infrastructure also hosts AWS Edge Locations. These locations are used by AWS CloudFront in order to deliver content at low latency to local clients requesting the data. There are many Edge Locations in North America; in fact, there are too many to list here.

AVAILABILITY ZONES



Be sure to remember these facts regarding Availability Zones:

- AZs consist of one or more discrete data centers—each with redundant power, networking, and connectivity—housed in separate facilities.
- These AZs enable you to operate production applications and databases that are more highly available, fault-tolerant, and scalable than would be possible from a single data center.

AWS provides you with the flexibility to place instances and store data within multiple geographic regions as well as across multiple Availability Zones within each region. Amazon designs each Availability Zone as an independent failure zone. This independence means that Amazon physically separates Availability Zones within a typical metropolitan region. Amazon chooses lower-risk floodplains in each region.

In addition to discrete uninterruptible power supplies (UPSs) and onsite backup generation facilities, AZs are each fed via different grids from independent utilities to further reduce single points of failure. AZs are all redundantly connected to multiple Tier-1 transit providers. Some AZs have their own power substations; in fact, as I write this, a majority are creating their own power!

CONNECTIONS

There are many options for transparent and effective connectivity to the AWS Global Infrastructure and any Virtual Private Clouds (VPCs) you might be implementing.



Direct Connect

AWS Direct Connect makes it easy to establish a dedicated network connection from your premises to AWS. Features are numerous and include the following:

- Establishment of private connectivity between AWS and your data center, office, or colocation environment; keep in mind that you typically work with an AWS partner data center, so privacy of the connection is still relative.
- Potential reduction of your network costs (through savings of the transfer-out fee).
- Potential increase in bandwidth throughput.
- Typically, a more consistent network experience than Internet-based connections.
- Use of 802.1Q VLANs that enable you to partition the connection into multiple virtual interfaces able to access different resources.

VPC Endpoints

A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by PrivateLink without requiring an Internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC do not require public IP addresses to communicate with resources in the service. Traffic between your VPC and the other service does not leave the Amazon network.

Endpoints are virtual devices. They are highly available VPC components that allow communication between instances in your VPC and services without imposing availability risks or bandwidth constraints on your network traffic.



There are two types of VPC endpoints: interface endpoints and gateway endpoints. You should create the type of VPC endpoint required by the supported service.

Interface Endpoints (Powered by AWS PrivateLink)

An interface endpoint is an elastic network interface with a private IP address that serves as an entry point for traffic destined to a supported service. The following services are supported:

- API Gateway
- CloudWatch

- CloudWatch Events
- CloudWatch Logs
- CodeBuild
- Config
- EC2 API
- Elastic Load Balancing API
- Key Management Service
- Kinesis Data Streams
- SageMaker Runtime
- Secrets Manager
- Security Token Service
- Service Catalog
- SNS
- Systems Manager
- Endpoint services hosted by other AWS accounts
- Supported AWS Marketplace partner services

Gateway Endpoints

A gateway endpoint is a gateway that is a target for a specified route in your route table, used for traffic destined to a supported AWS service. The following AWS services are supported:

- S3

- DynamoDB

VPC Peering

An AWS VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, with a VPC in another AWS account, or with a VPC in a different AWS region.

AWS uses the existing infrastructure of a VPC to create a VPC peering connection; it is neither a gateway nor a VPN connection, and does not rely on a separate piece of physical hardware. There is no single point of failure for communication or a bandwidth bottleneck. Figure 10-2 shows the configuration of a VPC peering in AWS.

The screenshot shows the AWS Management Console interface for creating a VPC peering connection. The browser address bar shows the URL: `https://console.aws.amazon.com/vpc/home?region=us-east-1#CreatePeeringConne`. The console header includes the AWS logo, navigation tabs for Services, Resource Groups, and a user profile for 'asequira' in the 'N. Virginia' region. The main content area is titled 'Create Peering Connection' and contains the following fields:

- Peering connection name tag:** A text input field with an information icon.
- Select a local VPC to peer with:**
 - VPC (Requester):** A dropdown menu with a refresh icon.
- Select another VPC to peer with:**
 - Account:** Radio buttons for 'My account' (selected) and 'Another account'.
 - Region:** Radio buttons for 'This region (us-east-1)' (selected) and 'Another Region'.
 - VPC (Acceptor):** A dropdown menu with a refresh icon.

At the bottom, there is a '* Required' label, a 'Cancel' button, and a 'Create Peering Connection' button. The footer contains the URL `https://console.aws.amazon.com/vpc/home#3fregion%3Dus-east-1%26...`, copyright information '© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved.', and links for 'Privacy Policy' and 'Terms of Use'.

Figure 10-2 Configuring a VPC Peering

ClassicLink

ClassicLink allows you to link your EC2-Classic instance to a VPC in your account, within the same region. This allows you to associate the VPC security groups with the EC2-Classic

instance, enabling communication between your EC2-Classic instance and instances in your VPC using private IPv4 addresses.

ClassicLink removes the need to make use of public IPv4 addresses or Elastic IP addresses to enable communication between instances in these platforms. It is available to all users with accounts that support the EC2-Classic platform and can be used with any EC2-Classic instance.

There is no additional charge for using ClassicLink. Standard charges for data transfer and instance usage apply.

Note

EC2-Classic instances cannot be enabled for IPv6 communication. You can associate an IPv6 CIDR block with your VPC and assign IPv6 addresses to resources in your VPC; however, communication between a ClassicLinked instance and resources in the VPC is over IPv4 only.

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the exercises here, [Chapter 16, “Final Preparation,”](#) and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. [Table 10-](#)

3 lists these key topics and the page numbers on which each is found.



Table 10-3 Key Topics for Chapter 10

Key Topic Element	Description	Page Number
List	Regions characteristics	
List	AZ characteristics	
Overview	AWS Direct Connect	

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

Region

Availability Zone

Direct Connect

VPC endpoint

VPC peering

ClassicLink

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. Describe the AWS Global Infrastructure, from the largest component to the smallest.
2. How does AWS decide on the location of Availability Zones inside a region?
3. What is the AWS component that permits you to allow traffic flows between your VPCs in your AWS account?

Chapter 11

Resources for Technology Support

This chapter covers the following subjects:

- **Documentation:** Excellent documentation covering every facet of AWS is available to you for free online. You do not even need an account to access this information. This section of the chapter gives you more information regarding this massive amount of content.
- **Discussion Forums:** This part of the chapter discusses the many forums available for assistance with AWS. Although many AWS employees are in the forums helping members, the idea behind these forums is for members to assist other members. Most often, this assistance is not coming from an AWS employee, but a seasoned pro who has been using AWS successfully for a lengthy period of time.

Chapter 14, “Account Structures for Billing and Pricing,” provides detailed information about the various support plans you can purchase from Amazon for AWS. This chapter discusses superb resources you can take advantage of completely free of charge. In fact, the AWS documentation does not even require an account with Amazon for access.

Same with the FAQs I will introduce you to in this chapter. This chapter also presents information regarding the discussion forums of AWS. These forums require an AWS account for access, but keep in mind that this account can be in the Free Tier.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. [Table 11-1](#) lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 11-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions
Creating Your Free Tier Account	1-2
Building a Web Server with the Free Tier	3-4

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly

guess skews your self-assessment results and might provide you with a false sense of security.

1. Which statement regarding the AWS documentation is false?

- a.** The AWS documentation is carefully categorized to assist your usage.
- b.** The documentation consists of user guides and references broken down by topic.
- c.** You cannot access the documentation of AWS without at least a Free Tier account.
- d.** The documentation is accessed online.

2. Which of the following resources is often a frequent source for exam questions and topics?

- a.** FAQs
- b.** IEEE standards docs
- c.** Wikipedia.org
- d.** NIST standards

3. What is required in order to post questions to the group in the official discussion forums of AWS?

- a.** No special requirement exists
- b.** An AWS account
- c.** The Enterprise support plan
- d.** The Desktop support plan

4. Which is not a major category of the AWS discussion forums?
- a. AWS Security Alerts
 - b. Amazon Web Services
 - c. German Forums
 - d. AWS Startups

FOUNDATION TOPICS

DOCUMENTATION

I am not being trite when I tell you that the AWS documentation is very good. It is an excellent mix of theory and practical step-by-step guides. You can find the AWS documentation at <https://docs.aws.amazon.com>.

At press time, the documentation features the following categories and topics:

- Guides and API References
 - Compute
 - Storage
 - Database
 - Developer Tools
 - Security, Identity & Compliance
 - Machine Learning

- Management & Governance
- Migration & Transfer
- Mobile
- Networking & Content Delivery
- Media Services
- Desktop & App Streaming
- Analytics
- Application Integration
- Business Applications
- Internet of Things
- Robotics
- Blockchain
- Game Development
- AR & VR
- Customer Engagement
- SDKs & Toolkits
- General Reference
- AWS Management Console
- Additional References
- Tutorials and Projects
 - Websites and Web Apps
 - DevOps

- Storage
- Database
- SDKs and Toolkits
- General Resources

Keep in mind that there are many different sections under the categories and topics from the preceding list. For example, in the Guides and API References category there is Compute. Inside the Compute documentation is Amazon EC2, Amazon EC2 Auto Scaling, and Migrate to Amazon EC2. Inside those topics you will find User Guides, API References, CLI References, and more. Figure 11-1 shows an example of just some of the resources located under **Guides and API References > Compute > Amazon EC2**.

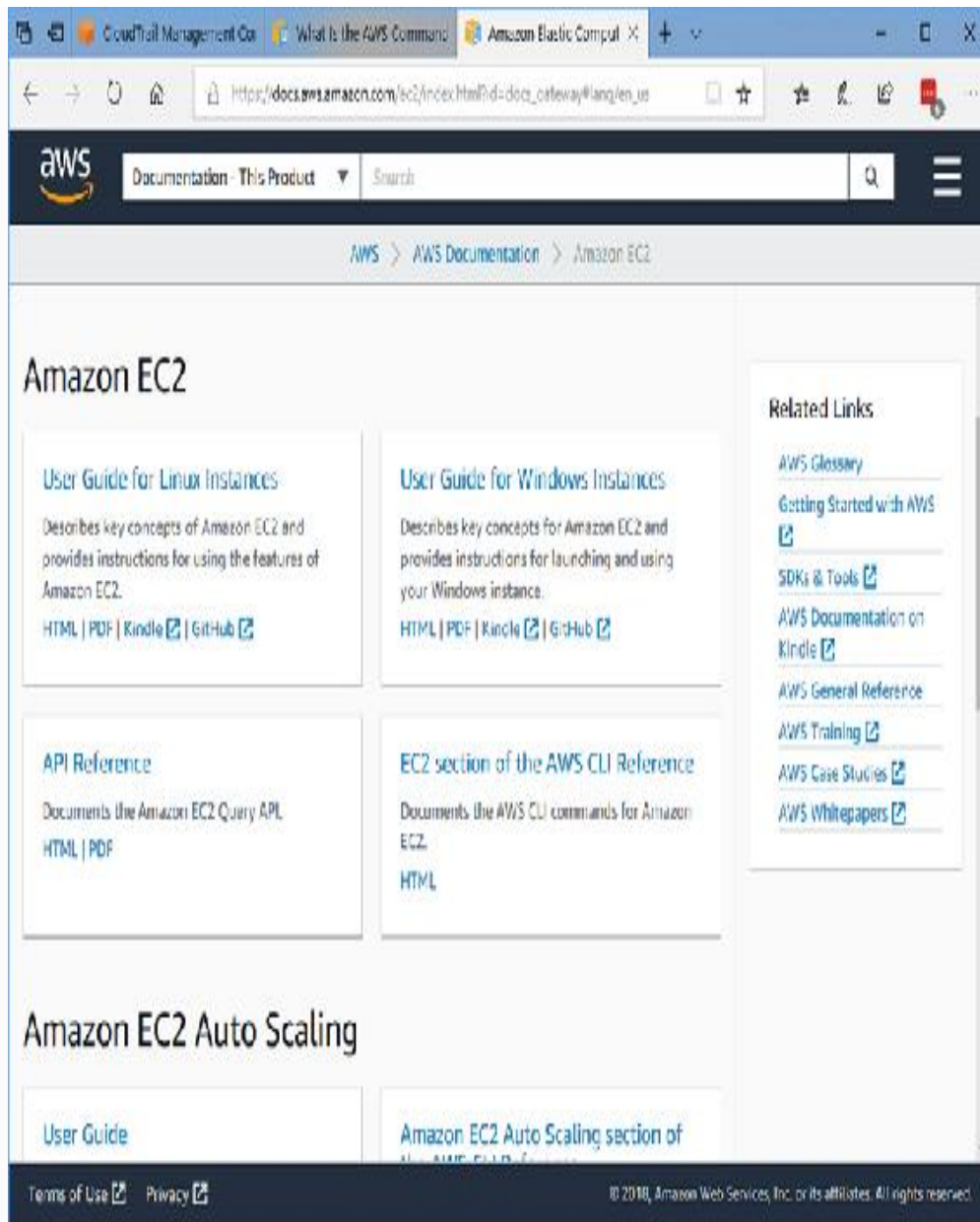


Figure 11-1 The AWS Online Documentation



Some of my all-time favorite resources are in the “related links” made available in sections. You will love sections like the following:

- AWS Glossary
- AWS Case Studies
- AWS Whitepapers
- AWS General Reference



Another excellent resource that Amazon makes available is FAQs. They are located at <https://aws.amazon.com/faqs>. These documents are also categorized and broken down by topic (for example, Machine Learning – AWS SageMaker FAQ).

Figure 11-2 shows you some of the subcategories found under the Amazon EC2 area.

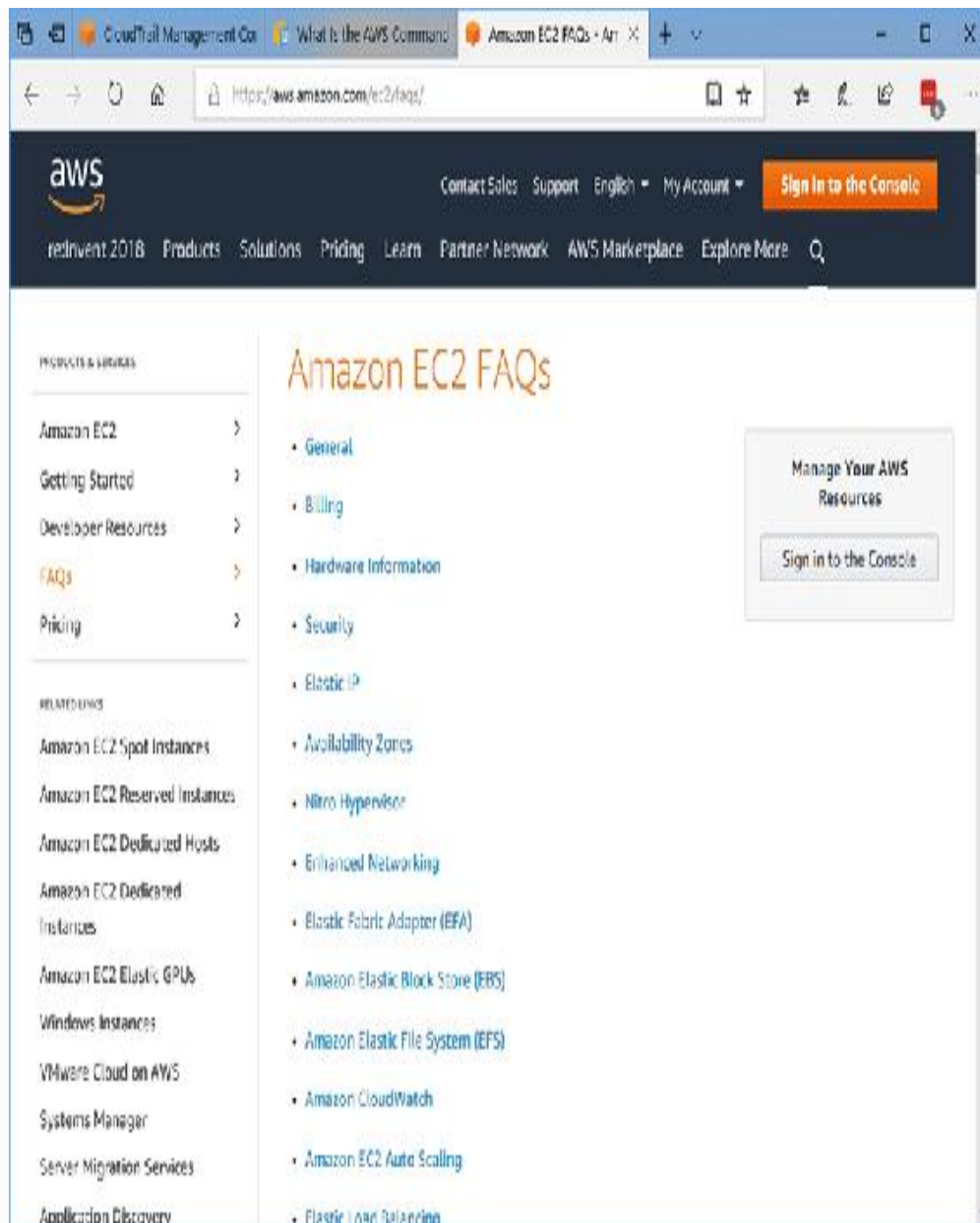


Figure 11-2 The FAQ Categories for EC2

For those of you interested in AWS certifications, understand that the exam authors love to draw question material from this excellent document. Reading FAQs is a fun way to learn very relevant aspects of the technologies and how they operate.

DISCUSSION FORUMS

Amazon hosts very effective (and very moderated) discussion forums. These forums are located at <https://forums.aws.amazon.com>.

You access the forums with an AWS login and can post questions or comments you have in one of the very targeted forums on the site. While most of us refer to the forums as “discussion forums,” as they are still titled to this day, be aware that many AWS materials refer to these forums as the “support forums.”

At press time, the forums are broken down as follows:

- Amazon Web Services
- AWS Startups
- AWS Web Sites and Resources
- Japanese Forums
- German Forums
- Portuguese Forums
- Korean Forums
- Indonesian Forums
- Other Topics

Keep in mind that these forums are divided into topics as well. So, for example, under the AWS Web Sites and Resources forum, you will discover topics like the following:

- General Feedback
- AQS Quick Start Reference Deployments
- Java Development
- Python Development
- And many more...

To help motivate responders, the forums award points to those members who are the most helpful.

Figure 11-3 shows an example of the forums available in this support area of AWS.

- Read the forum's rules and guidelines before posting for the first time.
- Search the other posts to see if your topic is already covered. I rarely discover that my question has not already been asked.
- Use a meaningful title for your thread.
- Do not use the forums to promote your product, service, or business.
- Be civil.
- Stay on topic.
- Do not submit a post that requires readers to download a large attachment. Either explain the attachment or, better yet, provide a link to the information.
- In order to be understood by most people, use correct spelling and grammar and avoid slang unless you know the word or phrase will be understood by other members.
- Do not double post (post the same message twice in one thread) or cross-post (place the same message across several forums).
- When replying to a post, do not quote more from the previous post than you have to.
- Do not post new problems on someone else's thread and interrupt a topic of discussion.
- Do not use someone else's thread for a private conversation.

- Do not post any information that you want private. Posts should not contain personal, identifiable information or content embarrassing to others.
- Do not post content that violates a copyright.
- Write concisely.
- Do not use words like “urgent” and “important” in your subject line. Be patient.
- Try and be kind to new members.

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the exercises here, [Chapter 16, “Final Preparation,”](#) and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. [Table 11-2](#) lists these key topics and the page numbers on which each is found.



Table 11-2 Key Topics for [Chapter 11](#)

Key Topic Element	Description	Page Number
List	Related topic links	
Overview	AWS FAQs	

Define Key Terms

There are no key terms for this chapter.

Q&A

The answers to these questions appear in [Appendix A](#). For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. Provide at least two examples of resource types found in the AWS documentation.
2. What is required in order to post on the AWS discussion forums?

Part IV

Domain 4: Billing and Pricing

Chapter 12

Using the Free Tier to Build a Web Server

This chapter covers the following subjects:

- **Creating Your Free Tier Account:** The Free Tier in AWS is an excellent way for you to get started with Amazon Web Services. In this section of the chapter, you get details about a Free Tier account and you perform a lab that sets you up with this service level.
- **Building a Web Server with the Free Tier:** This section of the chapter walks you through the steps required to build a web server in AWS using your Free Tier account.

It is important for you to understand the options around the Free Tier account in AWS. This chapter educates you on this powerful starting option. It also ensures you can use this account to create a fully functional web server in AWS.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. Table 12-1 lists the major headings in this chapter and the “Do I Know This Already?”

quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 12-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions
Creating Your Free Tier Account	1-2
Building a Web Server with the Free Tier	3-4

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1.** How long is the Free Tier period by default?
 - a. 2 years
 - b. 1 year
 - c. 6 months
 - d. 3 months
- 2.** Which is not an example of a service that remains free after the Free Tier expiration?

- a. SNS
 - b. Glacier
 - c. EC2
 - d. CloudWatch
3. What component related to an EC2 instance do you modify in order to permit the correct traffic forms?
- a. Security group
 - b. Container
 - c. VPC
 - d. Instance type
4. What is used to authenticate access to your EC2 instance?
- a. Lambda
 - b. PPTP
 - c. Key pairs
 - d. Telnet

FOUNDATION TOPICS

CREATING YOUR FREE TIER ACCOUNT

Although the exact terms of the Free Tier account could change at any time, let's start by looking at the incredible amount of resources you receive for free for 1 year. We will

follow this up with the components that remain free after the 1-year period.



Here are the “free for a year” components (notice for any services not covered elsewhere in this text, we provide some details on these services for you):

- **API Gateway:** One million API calls per month
- **Cloud Directory:** Fully managed, cloud-native directory-building service for data with multiple hierarchies; 1 GB of storage per month.
- **CloudFront:** 50 GB of data transfers out.
- **Comprehend:** Continuously trained and fully managed natural language processing (NLP); 50,000 units of text (5M characters) for each API per month.
- **Connect:** A simple-to-use, cloud-based contact center that scales to support any size business; 90 minutes per month of Amazon Connect usage.
- **EC2:** 750 hours per month.
- **EFS:** 5 GB of storage.
- **EBS:** 30 GB for any combination of general-purpose (SSD) or magnetic.
- **Elastic Container Registry:** 500 MB of storage per month.
- **Elastic Transcoder:** 20 minutes of audio transcoding.

- **ElastiCache:** 750 hours of cache.t2.micro Node usage.
- **Elasticsearch:** 750 hours per month of a single-AZ t2.micro.elasticsearch or t2.small.elasticsearch instance.
- **GameLift:** Simple, fast, cost-effective dedicated game server hosting; 125 hours per month of Amazon GameLift c4.large.gamelift On-Demand instance usage, plus 50 GB EBS general-purpose (SSD) storage
- **Lex:** Build voice and chat text chatbots; 10,000 text requests per month.
- **MQ:** Amazon MQ is a managed message broker service for Apache ActiveMQ; 750 hours of a single-instance mq.t2.micro broker per month.
- **Pinpoint:** Targeted push notifications for mobile apps; 5,000 free targeted users per month.
- **Polly:** Turn text into speech; 5 million characters per month.
- **RDS:** 750 hours per month of db.t2.micro database usage (applicable DB engines).
- **Rekognition:** Deep learning–based image recognition service; 5,000 images per month.
- **S3:** 5 GB of standard storage.
- **Sumerian:** Build and run virtual reality, augmented reality, and 3D applications; 50 MB published scene that receives 100 views per month for free in the first year.
- **Transcribe:** Add speech-to-text capability to your applications with automatic speech recognition; 60

minutes per month.

- **Translate:** Fast, high-quality, and affordable neural machine translation; 2 million characters per month.
- **Data Pipeline:** Orchestration for data-driven workflows; three low-frequency preconditions
- **Greengrass:** Three devices for free.
- **IoT:** 250,000 messages published or delivered per month.
- **IoT Device Management:** 50 remote actions per month.
- **OpsWorks for Chef Automate:** 7,500 node hours.
- **OpsWorks for Puppet Enterprise:** 7,500 node hours.
- **Trusted Advisor:** Four checks on performance and security.
- **ELB:** 750 hours per month shared between Classic and Application Load Balancers.

Here are the services that will remain free for you after the 1 year is up:

- **Chime:** A modern unified communications (UC) service that offers frustration-free meetings with exceptional audio and video; unlimited usage of Amazon Chime Basic.
- **CloudWatch:** Ten custom metrics and ten alarms.
- **Cognito:** 50,000 MAUs each month.
- **DynamoDB:** 25 GB of storage.
- **Glacier:** 10 GB of storage retrievals.

- **Macie:** Discover, classify, and protect data; 1 GB processed by the content classification engine.
- **SES:** Cost-effective email in the cloud; 62,000 outbound messages per month.
- **SNS:** One million publishes.
- **SQS:** One million requests.
- **SWF:** 10,000 activity tasks.
- **CodeBuild:** 100 build minutes.
- **CodeLimit:** Highly scalable, managed source control service; five active users per month.
- **CodePipeline:** One active pipeline per month.
- **Database Migration Service:** 750 hours of Amazon DMS Single-AZ dms.t2.micro instance usage.
- **Glue:** Simple, flexible, and cost-effective extract, transform, and load (ETL) service; one million objects stored in the AWS Glue Data Catalog.
- **Key Management Service:** 20,000 free request per month.
- **Lambda:** One million free request per month.
- **Step Functions:** Coordinate components of distributed applications; 4,000 state transitions per month.
- **Storage Gateway:** 100 GB free per account.
- **X-ray:** Analyze and debug your applications; 100,000 traces recorded per month.

Lab: Creating Your Free Tier Account



If you do not already have a Free Tier account with AWS, it is time for you to create one! Follow these steps:

Step 1. Search Google for AWS Free Tier. Select the link from Amazon for the Free Tier account.

Step 2. Click the **Create a Free Account** button, as shown in Figure 12-1.

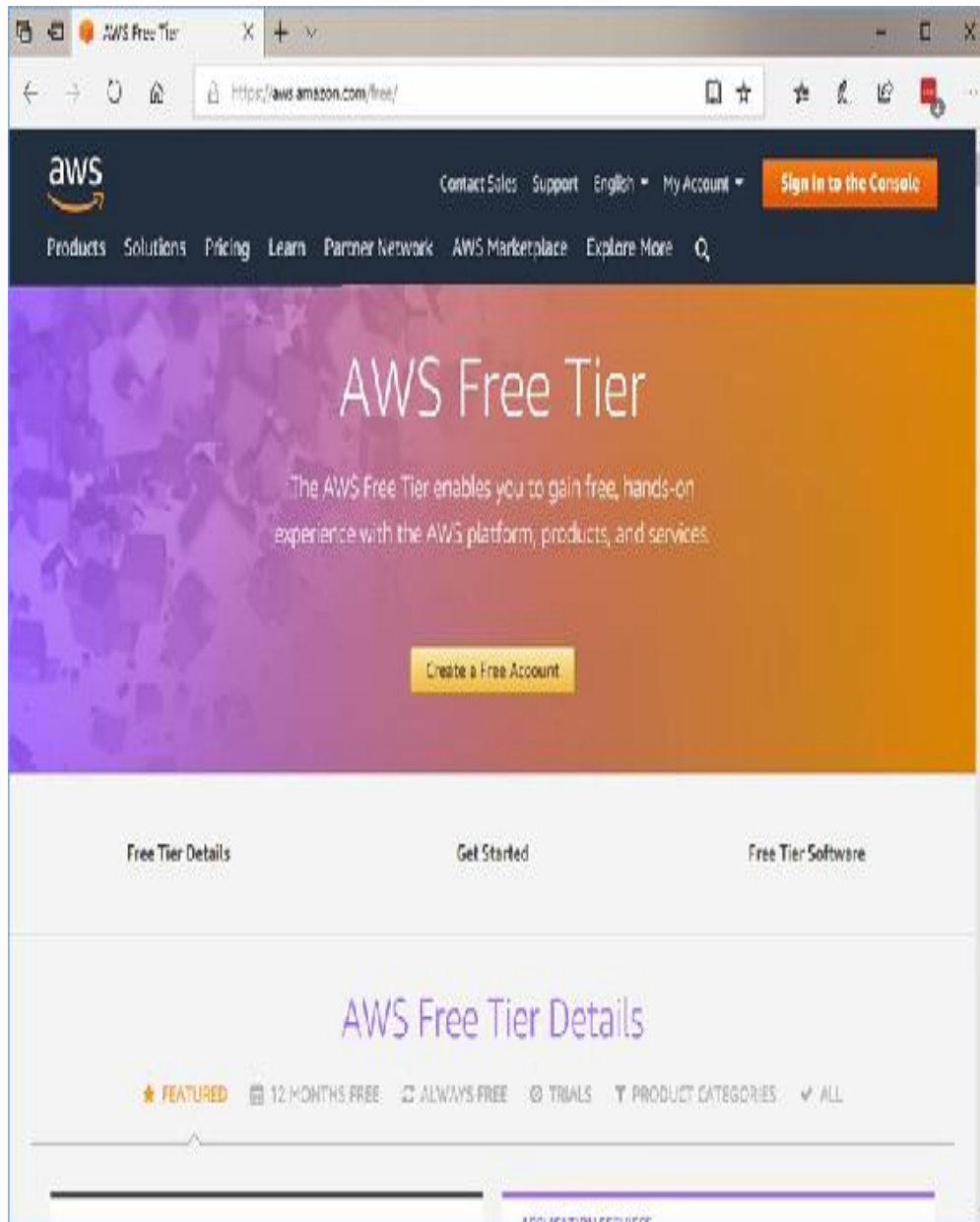


Figure 12-1 The Create a Free Account Button on the AWS Free Tier Page

Step 3. On the **Create an AWS Account** page (shown in Figure 12-2), provide your email address, password, and account name. The email address is critical and will be the username entry when you log in to this all-


powerful root account. The account name is how your account will display in AWS. This is not nearly as critical and can be changed at any time.


aws English


Create an AWS account


AWS Accounts Include 12 Months of Free Tier Access

Including use of Amazon EC2, Amazon S3, and Amazon DynamoDB
Visit aws.amazon.com/free for full offer terms

Email address 

Password 

Confirm password 

AWS account name 

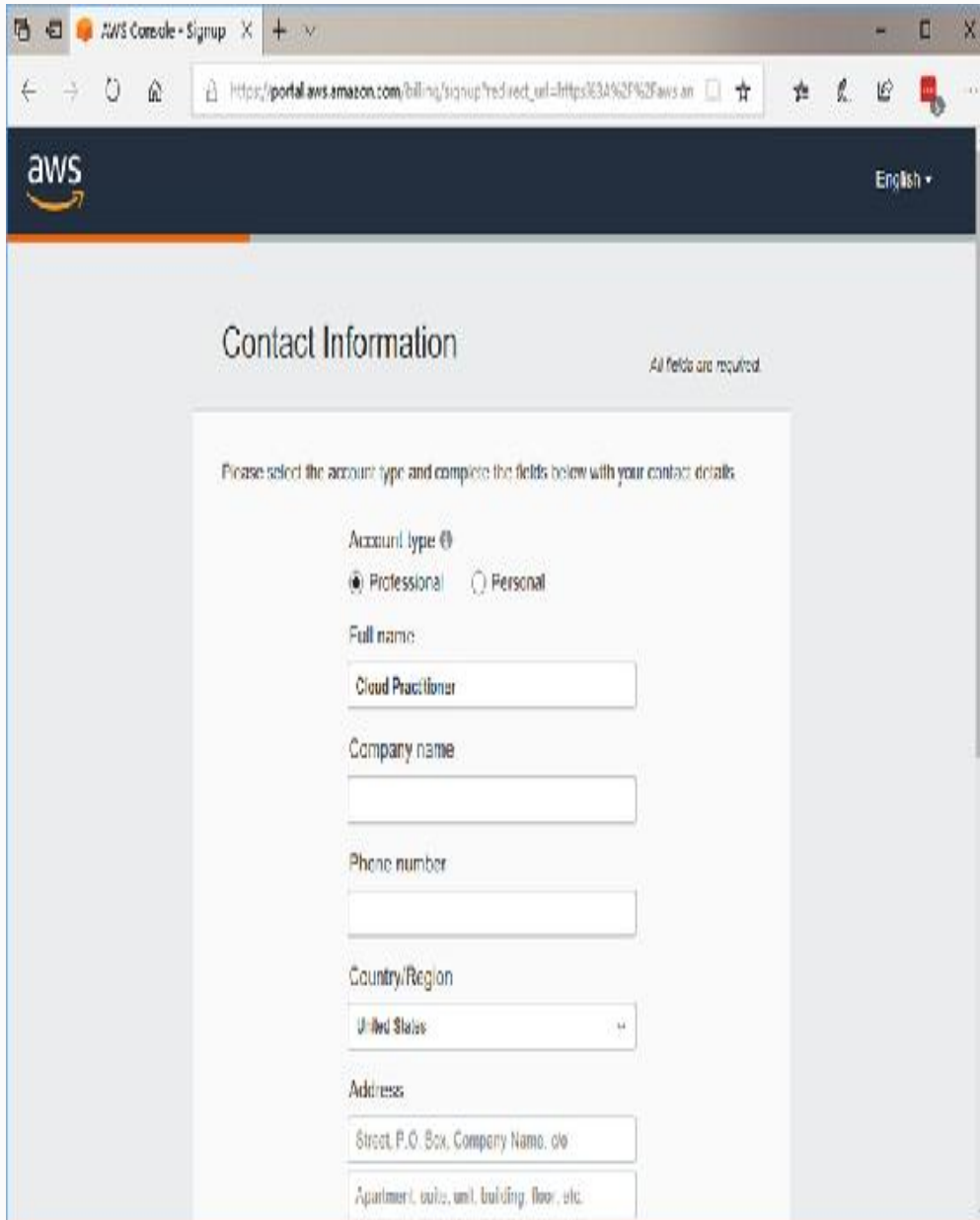
Continue

[Sign in to an Existing AWS Account](#)

© 2018 Amazon Web Services, Inc. or its affiliates. All rights reserved.
[Privacy Policy](#) [Terms of Use](#)

Figure 12-2 The Create an AWS Account Page

Step 4. Complete your basic contact information, as shown in Figure 12-3.

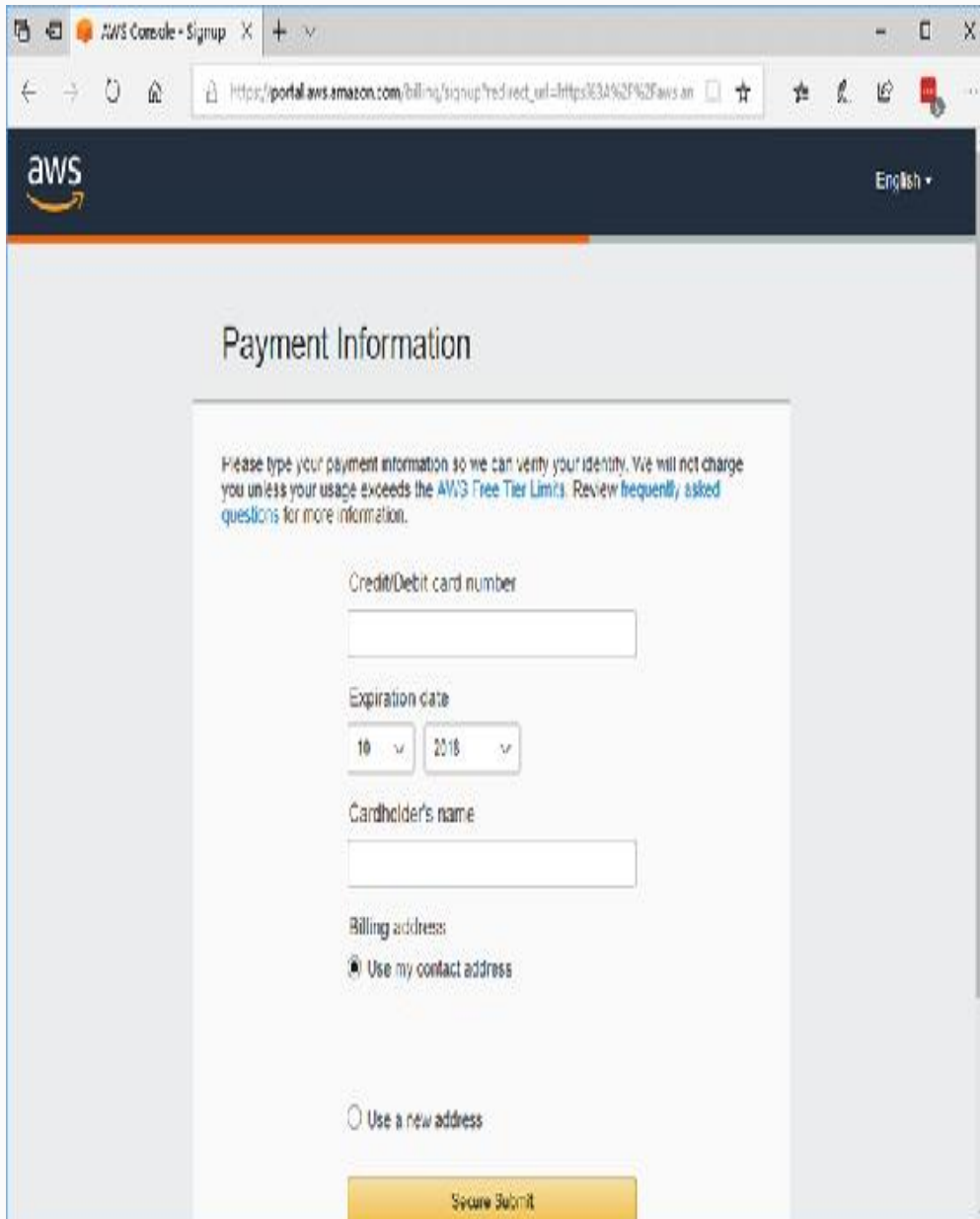


The screenshot shows a web browser window with the AWS Console Signup page. The browser's address bar displays the URL: `https://portal.aws.amazon.com/billing/signup?redirect_url=https%3A%2F%2Faws.amazon.com`. The page features the AWS logo in the top left and a language selector set to "English" in the top right. The main heading is "Contact Information", with a note stating "All fields are required." Below this, a sub-header reads: "Please select the account type and complete the fields below with your contact details." The form contains the following fields:

- Account type**: A radio button selection with "Professional" selected and "Personal" as an option.
- Full name**: A text input field containing the text "Cloud Practitioner".
- Company name**: An empty text input field.
- Phone number**: An empty text input field.
- Country/Region**: A dropdown menu currently showing "United States".
- Address**: Two stacked text input fields. The top field is labeled "Street, P.O. Box, Company Name, etc." and the bottom field is labeled "Apartment, suite, unit, building, floor, etc."

Figure 12-3 Providing Contact Information During Free Tier Signup

Step 5. Provide your payment information, as shown in [Figure 12-4](#). Note that you are not charged anything in the first year, as long as you do not exceed your Free Tier limits.

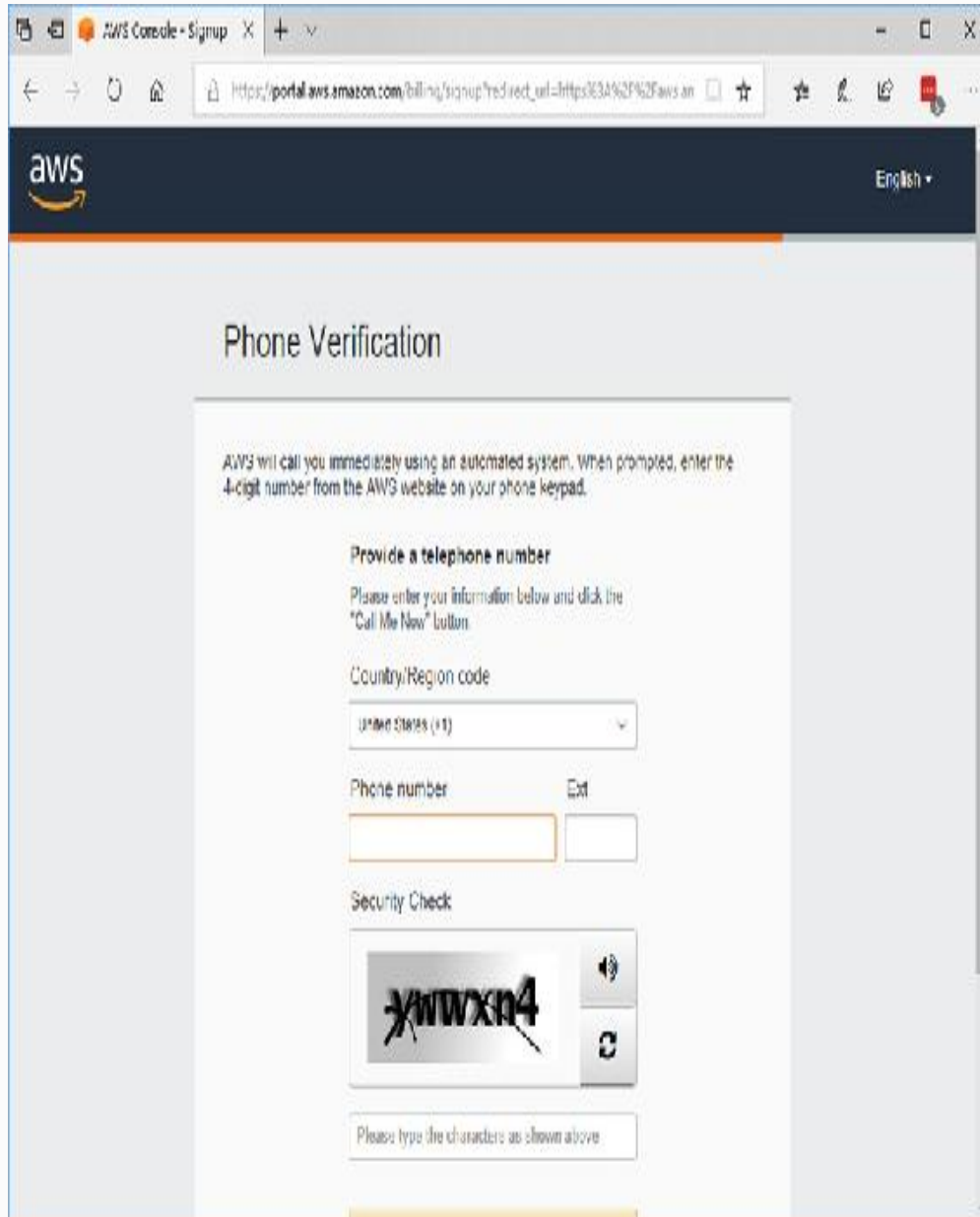


The screenshot shows a web browser window with the title "AWS Console - Signup". The address bar displays the URL "https://portal.aws.amazon.com/billing/signup?redirect_url=https%3A%2F%2Faws.amazon.com". The page features the AWS logo in the top left and a language selector set to "English" in the top right. The main heading is "Payment Information". Below this, a message states: "Please type your payment information so we can verify your identity. We will not charge you unless your usage exceeds the [AWS Free Tier Limits](#). Review [frequently asked questions](#) for more information." The form includes the following fields and options:

- Credit/Debit card number:** A single-line text input field.
- Expiration date:** Two dropdown menus showing "10" for the month and "2018" for the year.
- Cardholder's name:** A single-line text input field.
- Billing address:** Two radio button options: "Use my contact address" (which is selected) and "Use a new address".
- Secure Submit:** A yellow button at the bottom of the form.

Figure 12-4 Payment Information Screen in Free Tier Signup

Step 6. Provide the phone number for your phone verification and input the security check, as shown in [Figure 12-5](#).



The screenshot shows a web browser window with the AWS Console Signup page. The page title is "Phone Verification". Below the title, there is a message: "AWS will call you immediately using an automated system. When prompted, enter the 4-digit number from the AWS website on your phone keypad." Below this message, there is a section titled "Provide a telephone number". This section contains a prompt: "Please enter your information below and click the 'Call Me Now' button." Below the prompt, there is a "Country/Region code" dropdown menu with "United States (+1)" selected. Below the dropdown menu, there is a "Phone number" input field and an "Ext" input field. Below the phone number input field, there is a "Security Check" section. This section contains a CAPTCHA image showing the characters "ywwxn4" and a "Please type the characters as shown above" input field.

Figure 12-5 Phone Verification During Signup

Step 7. In the **Select a Support Plan** window, choose your support options, as shown in [Figure 12-6](#). Note that

there is only one free plan.

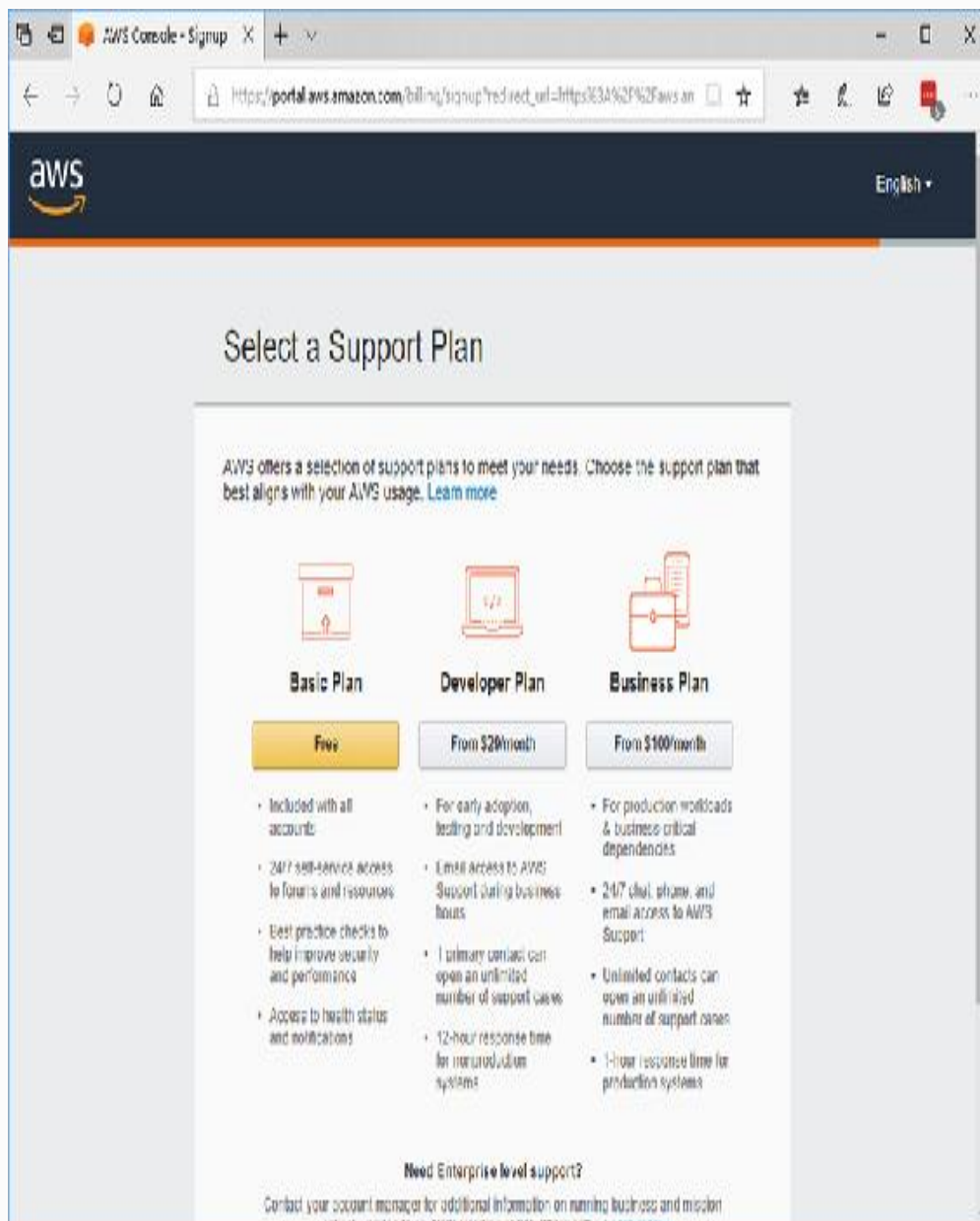


Figure 12-6 Selecting a Support Plan in the AWS Free Tier Signup

Step 8. Sign in to your new AWS account! Use the email address that you used for the account creation.

Remember, this is your root AWS account. You should use this account to create “normal” admin accounts for management of AWS. You should very rarely need to log in as this powerful root account. [Figure 12-7](#) shows the sign in page.



Figure 12-7 Time to Sign in to Your New Account!

Step 9. You are now ready to explore the wonders of AWS!

Figure 12-8 shows the welcome screen for the AWS Management Console.

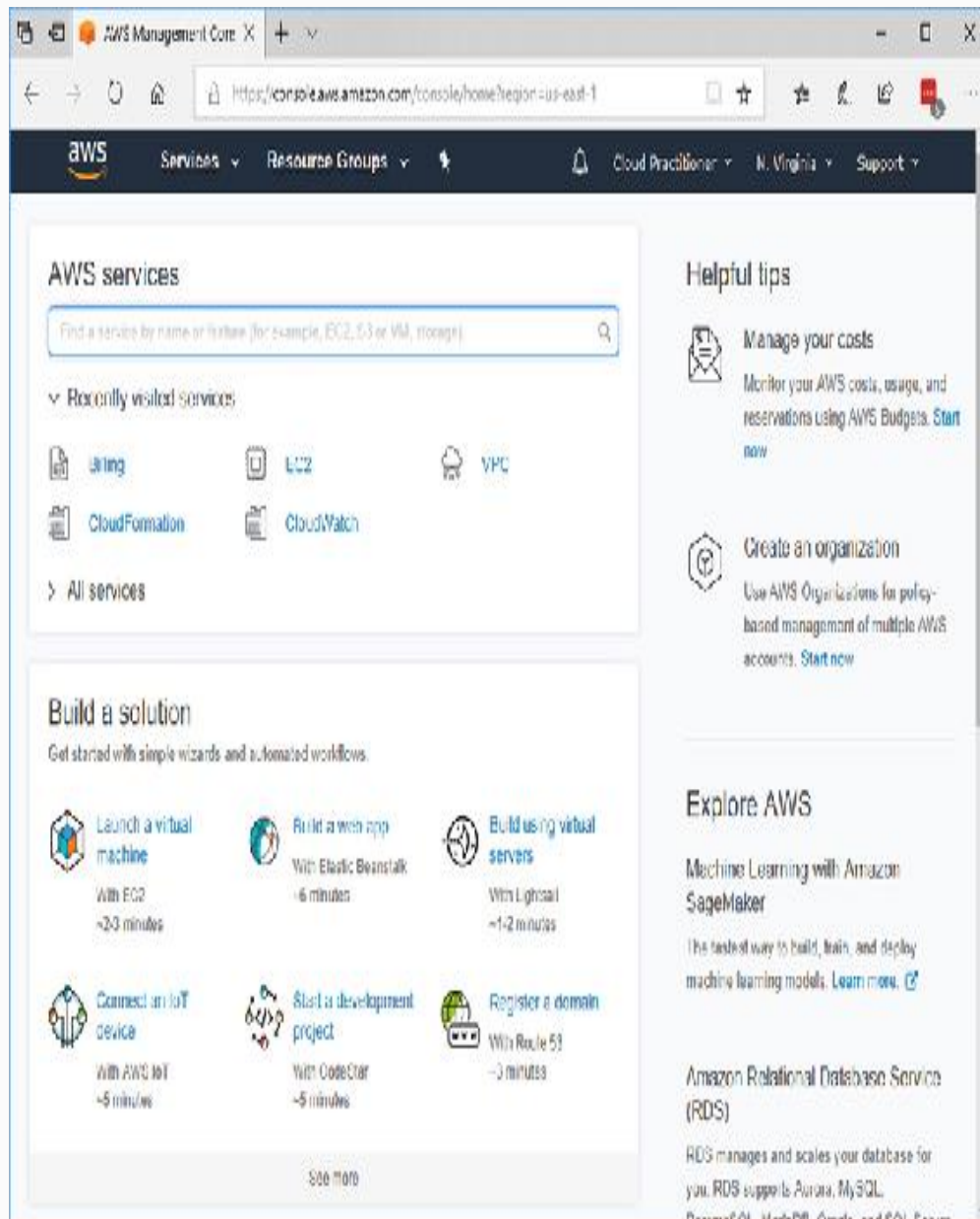


Figure 12-8 The AWS Management Console

Building a Web Server with the Free Tier

Now that you have your Free Tier account, it is time to have some fun and learn a bunch in the process! In this section, we build a fully functional web server in AWS using some simple steps. This lab demonstrates many of the technologies you are now familiar with thanks (in part) to this book. The lab builds a “LAMP” web server, which stands for an Apache web server with PHP and MariaDB (a community-developed fork of MySQL) support on an Amazon Linux 2 instance.

Lab: Building a Web Server with the Free Tier



Let’s walk through the steps required to build a free web server using AWS EC2:

- Step 1.** Search the AWS services for **EC2** and select the link to enter the **EC2 Dashboard**.
- Step 2.** Select **Launch Instance** to create a new EC2 instance for your cool web server.
- Step 3.** The **Choose an Amazon Machine Image (AMI)** page displays a list of basic configurations, called Amazon Machine Images (AMIs), that serve as templates for your instance. Select an HVM version of Amazon

Linux 2. Notice that these AMIs are marked “Free Tier eligible.”

Step 4. On the **Choose an Instance Type** page, you can select the hardware configuration of your instance. Select the **t2.micro** type, which is selected by default. Notice that this instance type is eligible for the Free Tier. Figure 12-9 shows this step.

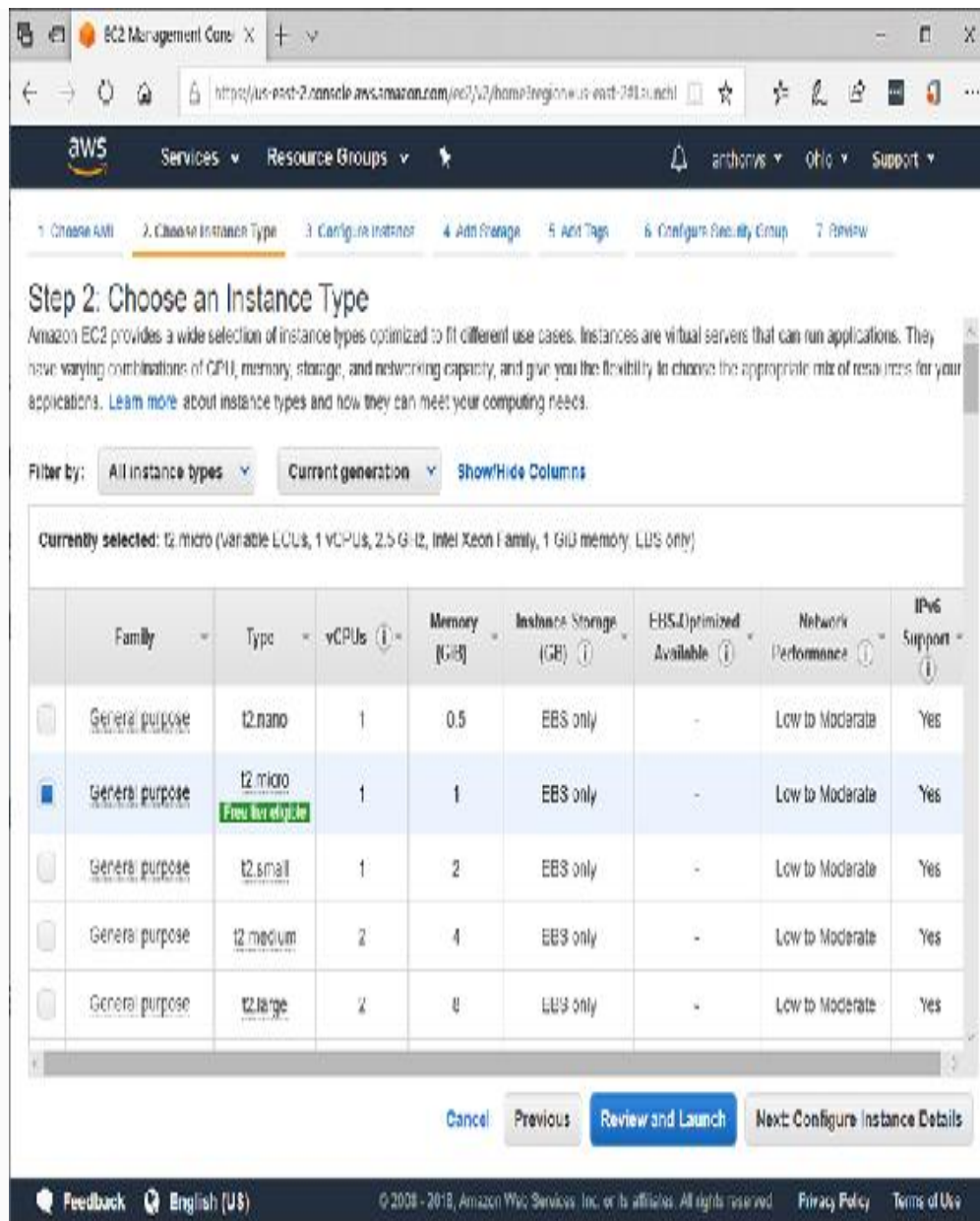


Figure 12-9 Choosing an Instance Type

Step 5. Choose **Review and Launch** to let the wizard complete the other configuration settings for you.

Step 6. On the **Review Instance Launch** page, under **Security Groups**, you'll see that the wizard created and selected a security group for you. You can use this

security group, or you can select the security group you created during setup using the following steps.

Step 7. Choose Edit security groups.

Step 8. Ensure your security group allows SSH (port 22), HTTP (port 80), and HTTPS (port 443) connections, as shown in [Figure 12-10](#).

The screenshot shows the AWS Management Console interface for the 'Configure Security Group' step of the EC2 instance launch wizard. The breadcrumb trail at the top indicates the steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group (current step), and 7. Review.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access

Feedback English (US) © 2018 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Figure 12-10 Ensuring Your Security Group Permits the
Correct Traffic

Step 9. Choose **Review and Launch**.

Step 10. On the **Review Instance Launch** page, choose **Launch**.

Step 11. When prompted for a key pair, select **Choose an existing key pair**, then select the key pair that you created previously. Alternatively, you can create a new key pair. Select **Create a new key pair**, enter a name for the key pair, and then choose **Download Key Pair**. This is the only chance for you to save the private key file, so be sure to download it. Save the private key file in a safe place. You'll need to provide the name of your key pair when you launch an instance and the corresponding private key each time you connect to the instance.

Step 12. When you are ready, select the acknowledgement check box and then choose **Launch Instances**.

Step 13. A confirmation page lets you know that your instance is launching. Choose **View Instances** to close the confirmation page and return to the console.

Step 14. Connect to your instance once it is ready—its status in the console will be **Running**. Use the **Connect** button for instructions on making your SSH connection.

Step 15. After logging in to your instance as the user account **ec2-user**, ensure that all of your software packages are up to date by performing a quick software update on your instance. This process may take a few minutes, but it is important to make sure that you have the latest security updates and bug fixes. Use the following command:

```
[ec2-user ~]$ sudo yum update -y
```

Step 16. Install the **lamp-mariadb10.2-php7.2** and **php7.2** Amazon Linux Extras repositories to get the latest versions of the LAMP MariaDB and PHP packages for Amazon Linux 2. Use the following command:

```
[ec2-user ~]$ sudo amazon-linux-extras install -y  
lamp-mariadb10.2-php7.2 php7.2
```

Step 17. Now that your instance is current, you can install the Apache web server, MariaDB, and PHP software packages. Use the **yum install** command to install multiple software packages and all related dependencies at the same time:

```
[ec2-user ~]$ sudo yum install -y httpd mariadb-  
server
```

Step 18. Start the Apache web server:

```
[ec2-user ~]$ sudo systemctl start httpd
```

Step 19. Use the **systemctl** command to configure the Apache web server to start at each system boot:

```
[ec2-user ~]$ sudo systemctl enable httpd
```

Step 20. Test your web server. In a web browser, type the public DNS address (or the public IP address) of your instance. If there is no content in `/var/www/html`, you should see the Apache test page. You can get the public DNS for your instance using the Amazon EC2 console (check the Public DNS column; if this column is hidden, choose **Show/Hide Columns** [the gear-shaped icon] and choose **Public DNS**).

Step 21. Its time to shut down your handy LAMP web server. Issue the following command:

```
[ec2-user ~]$ sudo shutdown -h now
```

NOTE

You can also shut down instances using the AWS Management Console with the EC2 Dashboard. I always prefer to shut systems down from their own interface when I am working within them.

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the exercises here, Chapter 16, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 12-

2 lists these key topics and the page numbers on which each is found.



Table 12-2 Key Topics for Chapter 12

Key Topic Element	Description	Page Number
List	Free Tier components	
Lab	Creating a Free Tier account	
Lab	Creating a web server with the free tier	

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

Free Tier

Q&A

The answers to these questions appear in [Appendix A](#). For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. Provide at least three examples of Free Tier services that can remain forever free.

2. Why might you shut down your EC2 instances in AWS when practicing with the Free Tier account?

Chapter 13

AWS Pricing Models

This chapter covers the following subjects:

- **Fundamentals of Pricing:** This section describes how pricing works in AWS in general. It educates you on the fundamental types of costs associated with using AWS.
- **Pricing Details:** This section ensures you understand the various factors that go into pricing for a given service. This section is critical for you to be able to control your costs in AWS.

AWS can save you money, in addition to the many other advantages that this public cloud offering can bring. However, you can most effectively save money only if you understand the pricing model in general as well as the various factors that go into charges for the main services of AWS. This chapter ensures you have this knowledge. Although not every service is covered in this chapter, knowing these variables and seeing some examples will help you understand how other services may be charged for.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. [Table 13-1](#) lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 13-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions
Fundamentals of Pricing	1-2
Pricing Details	3-4

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1.** Which is not an example of a service that is always free?
 - a.** IAM
 - b.** Auto Scaling
 - c.** CloudFormation
 - d.** EC2

2. Which of the following is not a type of EC2 purchase plan?

- a. On-Demand
- b. Virtual-Only
- c. Reserved
- d. Spot

3. Which is not a fundamental cost in AWS?

- a. Data transfer in
- b. Data transfer out
- c. Storage
- d. Compute

4. Which is not a common cost characteristic for EC2?

- a. Clock hours
- b. Detailed monitoring
- c. AZ location
- d. Hardware options

FOUNDATION TOPICS

FUNDAMENTALS OF PRICING



Remember, the general concept of the pricing in AWS follows the utility company model. Furthermore, AWS pricing follows these general concepts:

- **Pay as you go:** This is done without excessive long-term commitments. It ensures adaptability and helps to eliminate CapEx costs for IT. Costs are related to cheaper variable costs as you operate. Figure 13-1 shows some sample costs associated with an EC2 instance.

F5 BIG-IP Virtual Edition - BEST (PAYG, 200Mbps)

Product Details

- By: F5 Networks
- Customer Rating: ***** (0)
- Latest Version: 14.0.0.1-0.0.2
- Base Operating System: Linux/Unix, CentOS 6.0
- Delivery Method: 64-bit Amazon Machine Image (AMI)
- License Agreement: [End User License Agreement](#)
- On Marketplace Since: 1/25/10
- AWS Services Required: Amazon EC2, Amazon EBS, Amazon VPC
- Highlights:

Pricing Details

Free Trial!
Try one instance of this product for 30 days. There will be no software charges but AWS infrastructure charges will still apply. Your Free Trial will automatically convert to a paid subscription upon expiration.

Hourly Fees

Instance Type	Software	EC2	Total
M3 Extra Large	\$2.50	\$0.266	\$2.766/hr
M5 Extra Large	\$2.50	\$0.192	\$2.692/hr
M4 Extra Large	\$2.50	\$0.20	\$2.70/hr
C1 Quaduple Extra Large	\$2.50	\$0.84	\$3.34/hr
T2 Large	\$2.50	\$0.093	\$2.593/hr
C4 Double Extra Large	\$2.50	\$0.390	\$2.890/hr
M5 Large	\$2.50	\$0.096	\$2.596/hr
C4 Large	\$2.50	\$0.085	\$2.585/hr
M5 Double Extra Large	\$2.50	\$0.304	\$2.804/hr
CC2 Cluster Compute	\$7.50	\$2.00	\$4.50/hr
C4 Eight Extra Large	\$2.50	\$1.591	\$4.091/hr
M4 Quaduple Extra Large	\$2.50	\$0.80	\$3.30/hr
M5 12 Extra Large	\$2.50	\$2.304	\$4.804/hr
T2 Medium	\$2.50	\$0.046	\$2.546/hr

[View Additional Details in AWS Marketplace](#)

[More info](#)

[Cancel](#) [Continue](#)

Figure 13-1 Sample EC2 Instance Costs

NOTE

Notice how there is a 30-day free trial for this sample EC2 instance. This way, you get to spin it up and ensure it works for you before you start paying for usage. This is common with many EC2 instances in the AWS Marketplace in the Management Console.

- **Pay less when you reserve:** You can use reserved EC2 instances and save as much as 70% over On-Demand pricing; you can pay all up front, pay some up front, or pay nothing up front for these reserved instances. Discounts vary, as you pay less up front. Remember, there is also spot pricing, where you can bid an amount you are willing to pay for compute power. Figure 13-2 shows an example of reserved instance pricing for a Windows Server running SQL Server Enterprise Edition on a instance type called a t3.xlarge. As you might guess, these systems are packed with horsepower.

Purchase Reserved Instances

Platform: Windows Server Tenancy: Default Offering Class: Any
 Instance Type: t3.xlarge Term: Any Payment Option: Any

Seller	Term	Effective Rate	Upfront Price	Hourly Rate	Payment Option	Offering Class	Quantity Available
AWS	12 months	\$1.678	\$0.00	\$1.678	No Upfront	standard	Unlimited
AWS	12 months	\$1.694	\$0.00	\$1.694	No Upfront	convertible	Unlimited
AWS	36 months	\$1.546	\$0.00	\$1.546	No Upfront	standard	Unlimited
AWS	36 months	\$1.556	\$0.00	\$1.556	No Upfront	convertible	Unlimited
AWS	12 months	\$1.673	\$7,328.00	\$0.837	Partial Upfront	standard	Unlimited
AWS	12 months	\$1.688	\$7,393.00	\$0.844	Partial Upfront	convertible	Unlimited
AWS	12 months	\$1.871	\$14,638.00	\$0.000	All Upfront	standard	Unlimited
AWS	12 months	\$1.586	\$14,756.00	\$0.000	All Upfront	convertible	Unlimited

You currently have no items in your cart.

Figure 13-2 Sample Reserved Instance Pricing

- **Pay even less per unit by using more:** Services like S3 and EC2 offer volume discounts as your AWS infrastructure grows.
- **Pay even less as AWS grows:** Amazon is constantly learning how to host the cloud more efficiently; as they

save costs, they pass these savings on to you.

If you are a very large enterprise, realize that Amazon can also offer custom pricing models. This might be required if you have a very large volume project and their pricing model would be cost prohibitive.

Also, remember the Free Tier of service that you can start with. Keep in mind that some services of AWS can remain free (given certain service levels). These free services include the following:

- VPC
- CloudFormation
- IAM
- Auto Scaling

PRICING DETAILS



It is important that you memorize the general cost categories of AWS:

- Compute
- Storage
- Data Transfer Out (aggregated across services)

Notice that, in general, there are no charges for the following:

- Data transfers in
- Data transfers between AWS resources



What are the variables that go into the pricing of the different fundamentals services? Here are some to give you a feel for your abilities to control costs:

- **EC2:** Total clock hours of usage; amount and distribution of load balancing; machine configuration; detailed monitoring; machine purchase type; software/OS; elastic IP addresses; number of instances (including those created by Auto Scaling); cross-AZ data transfer
- **S3:** Storage type; storage class; requests; data transfer out
- **EBS:** Volume type; IOPS; snapshots
- **RDS:** Total clock hours of usage; additional storage; database configuration; purchase type; deployment type; number of databases; data transfer out; provisioned storage
- **CloudFormation:** Traffic distribution location; request; data transfer out

Remember, you can also obtain up-to-the-second details on your AWS costs thanks to the cost tools available in the AWS Management Console. Figure 13-3 shows an example of a quick cost report.

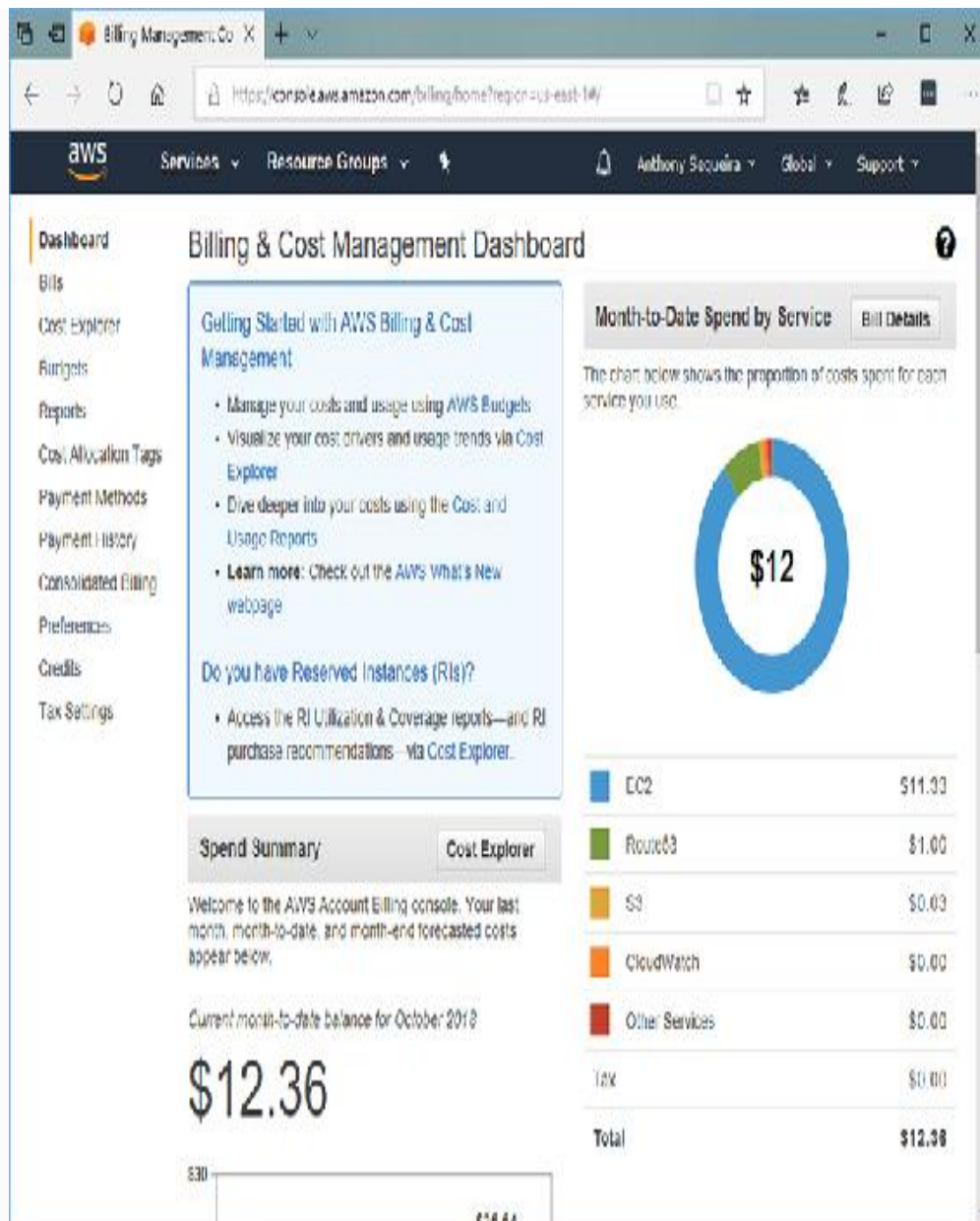


Figure 13-3 Checking AWS Costs

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the

exercises here, Chapter 16, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 13-2 lists these key topics and the page numbers on which each is found.



Table 13-2 Key Topics for Chapter 13

Key Topic Element	Description	Page Number
List	General pricing rules of AWS	
List	Fundamentals of pricing	
List	Typical cost variables for common services	

Define Key Terms

There are no key terms in this chapter.

Q&A

The answers to these questions appear in [Appendix A](#). For more practice with exam format questions, use the Pearson

Test Prep Software Online.

- 1.** Name at least two fundamental cost areas of AWS.

- 2.** Name at least two cost variables for AWS S3.

Chapter 14

Account Structures for Billing and Pricing

This chapter covers the following subjects:

- **AWS Support Plans Overview:** What are the goals behind the Amazon support team for AWS customers? This section discusses this topic as well as provides examples of specific tools you have access to for support help.
- **Comparing the Plans:** This section of the chapter provides a valuable comparison of the various support plans you can purchase.

Let's face it. No matter how long you have been working with AWS, at some point you might require support assistance from an Amazon employee. This chapter provides you with an overview of how support works in AWS. It also provides you with a detailed breakdown of the different support options so you can begin thinking about the best plan for your AWS implementation.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. [Table 14-1](#) lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 14-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions
AWS Support Plans Overview	1-2
Comparing the Plans	3-4

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1.** What service in AWS allows core checks to be performed by any customer regardless of their support plan level?
 - a.** CloudFront
 - b.** CloudFormation
 - c.** CloudTrail

- d. Trusted Advisor**
- 2.** Who can act as a dedicated voice for you within AWS and serve as your technical point of contact and advocate?
 - a. Cloud Practitioner**
 - b. Primary Solution Architect**
 - c. TAM**
 - d. Concierge**
- 3.** What two support plans offer response times of 1 hour or less?
 - a. Developer**
 - b. Enterprise**
 - c. Business**
 - d. Basic**
- 4.** What minimal level of support gives you access to a TAM?
 - a. Business**
 - b. Basic**
 - c. Enterprise**
 - d. Developer**

FOUNDATION TOPICS

AWS SUPPORT PLANS OVERVIEW

Amazon provides a rich set of AWS resources as well as human resources to assist you within AWS. As you will see in the next section, there are different plans you can invest in to try and match your needs and your budget with a plan that makes sense for your organization.



AWS support centers around these goals:

- **Proactive guidance:** Your support plan might include access to a Technical Account Manager (TAM). The TAM is your primary point of contact who provides guidance, architectural review, and ongoing communication to keep you informed and well prepared as you plan, deploy, and proactively optimize your solutions. The TAM offers the following:
 - A dedicated voice within AWS to serve as your technical point of contact and advocate
 - Proactive guidance and best practices to help optimize your AWS environment
 - Orchestration and access to the breadth and depth of technical expertise across the full range of AWS
- **Best practices:** One of the valuable support resources is AWS Trusted Advisor, as shown in [Figure 14-1](#). This is an online resource that helps you provision your resources following best practices to help reduce cost, increase performance and fault tolerance, and improve security by

optimizing your AWS environment. As you learn in the next part of this chapter, four core checks are available to all AWS customers. The full power of AWS Trusted Advisor is available with Business and Enterprise support plans. Trusted Advisor offers the following:

- Guidance on getting the optimal performance and availability based on your requirements
- Opportunities to reduce your monthly spend and retain or increase productivity
- Best practices to help increase security



Figure 14-1 Trusted Advisor in AWS

- **Account assistance:** Included as part of the Enterprise support plan, the Concierge team is composed of AWS billing and account experts who specialize in working with enterprise accounts. This Concierge team will quickly and efficiently assist you with your billing and account inquiries, and work with you to implement billing and account best practices. Concierge support includes the following:

- 24×7 access to AWS billing and account inquiries
- Guidance and best practices for billing allocation, reporting, consolidation of accounts, and root-level account security
- Access to Enterprise account specialists for payment inquiries, training on specific cost reporting, assistance with service limits, and facilitating bulk purchases
- **Launch support:** For planned events, including advertising and product launches, promotions, and infrastructure migrations where a significant increase in demand for your resources is expected, Infrastructure Event Management (IEM) delivers a highly focused engagement to provide architectural and scaling guidance. This tool aligns real-time operational resources to support the success of your event. IEM is included with Enterprise support and is available for an additional fee with Business support plans. It includes the following:
 - Event planning and preparation based on your use case and objectives
 - Resource recommendations and deployment guidance based on anticipated capacity needs
 - Dedicated attention from your AWS support team during your event
 - Guidance and support as you scale resources to normal operating levels post-event

COMPARING THE PLANS

Clearly, you should match your expected support needs with the plan that makes the most sense for you. In order to do that, you should use Table 14-2 carefully in order to make the correct choice. Please keep in mind that this table reflects the details at the time of this writing. To see the latest values, just to ensure there are not any major changes, be sure to visit <https://aws.amazon.com/premiumsupport/compare-plans>.



Table 14-2 The Various Support Plans of AWS

	Basic	Developer	Business	Enterprise
Support forums	Yes	Yes	Yes	Yes
Trusted Advisor	Seven core checks	Seven core checks	Full access	Full access
Health status	Personal Health Dashboard	Personal Health Dashboard	Personal Health Dashboard and Health API	Personal Health Dashboard and Health API
Tech support		Business hours email	24[ts]7 via email, chat, and phone	24[ts]7 via email, chat, and phone with Senior Cloud Engineer
Who can open cases		One primary contact	Unlimited contacts	Unlimited contacts
Best response times		12 hours	1 hour	15 minutes
Architecture support		General guidance	Contextual guidance	Review
Launch support			Infrastructure Event Management for a fee	Infrastructure Event Management
Programmatic case management			AWS Support API	AWS Support API
Third-party software support			Guidance and troubleshooting	Guidance and troubleshooting
Architecture review				Well-architected review
Operations support				Operational recommendations
Training				Online self-paced labs
Account assistance				Concierge support team
Proactive guidance				Designated Technical Account Manager
Pricing	Included free	Starts at \$29 per month	Starts at \$100 per month	Starts at \$15K per month

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the exercises here, Chapter 16, “Final Preparation,” and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. Table 14-3 lists these key topics and the page numbers on which each is found.



Table 14-3 Key Topics for Chapter 14

Key Topic Element	Description	Page Number
List	AWS support goals	
Table 14-2	AWS support plans	

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

Basic support plan

Developer support plan

Business support plan

Enterprise support plan

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. What are the four major goals of AWS support?
2. What are the four support plans of AWS?

Chapter 15

Resources for Billing Support

This chapter covers the following subjects:

- **Cost Calculators:** You might be wondering just how much money you can save by migrating to an AWS implementation. The TCO calculators can help dramatically with this important question. But these powerful tools are not the only calculators you have access to with AWS. This part of the chapter covers these options with you.
- **AWS Billing and Cost Management:** This part of the chapter discusses best practices in billing and cost management.

AWS is not going to be well received in your enterprise if you cannot afford it, or if it does not provide the cost savings that were expected. This chapter helps you achieve the cost controls you will want with AWS. It does this by sharing tools and best practices you should consider using in the areas of costs and billing.

“DO I KNOW THIS ALREADY?” QUIZ

The “Do I Know This Already?” quiz allows you to assess if you should read the entire chapter. [Table 15-1](#) lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the “Do I Know This Already?” quiz appear in [Appendix A](#).

Table 15-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundations Topics Section	Questions
Cost Calculators	1–2
AWS Billing and Cost Management	3–4

Caution The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

- 1.** Which of the following are cost calculators found in AWS? (Choose two.)
 - a.** TCO calculators
 - b.** AWS Fee Estimator
 - c.** AWS Cost Comparison Calculator

- d. AWS Simple Monthly Calculator**
- 2.** What type of billing does Amazon engage in for AWS?
 - a. Pay-as-you-terminate**
 - b. Pay-for-reservations**
 - c. Pay-as-you-go**
 - d. Pay-as-you-estimate**
- 3.** Why does AWS guarantee your exchange rate with AWS Billing and Cost Management?
 - a. In order to ensure that any refunds use the same exchange rate as your original transaction**
 - b. To save you costs**
 - c. To minimize the number of transactions in the system**
 - d. To optimize your costs for resources**
- 4.** The Budgets tool in AWS uses what component for visualization?
 - a. Cost Explorer**
 - b. Excel**
 - c. Tableau**
 - d. AWS GraphSage**

FOUNDATION TOPICS

COST CALCULATORS

When you are dealing with costs, it is great to have calculators and other tools that can assist you in estimating and planning. Fortunately, Amazon realized your needs here and provides several.

The Total Cost of Ownership (TCO) Calculators

AWS helps you reduce total cost of ownership (TCO) by reducing the need to invest in large capital expenditures (CapEx). AWS also offers a pay-as-you-go model that empowers you to invest in the capacity you need and use it only when the business requires it.

Amazon provides TCO calculators that allow you to estimate the cost savings when using AWS. These calculators also provide a detailed set of reports that can be used in executive presentations.

Finally, the calculators also give you the option to modify assumptions that best meet your business needs.



Using the AWS TCO calculators, you can do the following:

- Use the calculators to compare the cost of your applications in an on-premises or traditional hosting environment to AWS.
- Describe your on-premises or hosting environment configuration to produce a detailed cost comparison with

AWS.

- Get an instant summary report that shows you the 3-year TCO comparison by cost categories.
- Download a full report, including detailed cost breakdowns, methodology, assumptions, and FAQs; you can also store the report in AWS for easy sharing with others.

AWS Simple Monthly Calculator

Long before the creation of the set of TCO calculators, AWS provided us with the Simple Monthly Calculator. While many no longer use it, as they consider it replaced by the new tools, it still functions and is still very valuable.

The AWS Simple Monthly Calculator is a JavaScript-based tool that allows you to calculate your monthly cost for using Amazon S3, Amazon EC2, and Amazon SQS. This tool incorporates the latest pricing changes, including the tiered pricing model for download bandwidth. You can use this tool to estimate your monthly bill, to determine your best- and worst-case scenarios, and identify areas of development to reduce your monthly costs and even compare them with other service providers who do not offer pay-as-you-go billing.

The following lab demonstrates the use of the AWS Simple Monthly Calculator to estimate costs in AWS S3.

Lab: Estimating AWS S3 Costs

If you are interested in how you can use the AWS Simple Monthly Calculator to estimate costs in AWS, follow these steps:

Step 1. Use Google or your favorite search engine to search for **AWS Simple Monthly Calculator**. Click the link to access the online calculator. Figure 15-1 show the AWS Simple Monthly Calculator's main page.

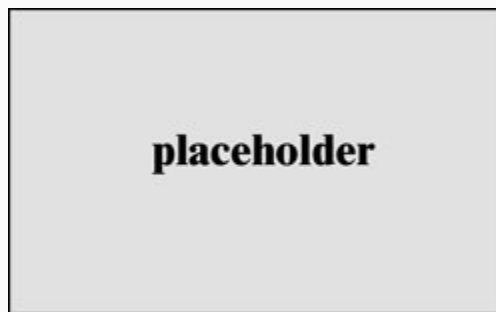


Figure 15-1 The AWS Simple Monthly Calculator

Step 2. On the left side, click the Amazon S3 link.

Step 3. Amazon S3 costs can vary by region. Select the **US West (Oregon)** region from the drop-down menu. Also, above this area, make sure that **Free Tier** is unchecked. This will give you estimates that do not include any Free Tier levels of access.

Step 4. Under **S3 Standard Storage & Requests**, enter **800 GB** as an example. The amount of your estimated monthly charge for this storage appears in a tab near the top of the interface. In this example (yours might vary because AWS charges also vary over time), this results in approximately \$18.40 per month in fees.

Step 5. Choose the **Clear Form** button to clear this entry.

Step 6. To examine how to save if you choose a different S3 storage tier, under the **S3 One Zone-Infrequent Access (S3 One Zone-IA) Storage & Requests** field, enter **800 GB** and examine the result. In this case, the result is just \$8 per month!

AWS BILLING AND COST MANAGEMENT

AWS Billing and Cost Management is the service you use to pay your AWS bill, monitor your usage, and budget your costs. AWS automatically charges the credit card you provided when you signed up for a new account with AWS. Charges appear on your credit card bill monthly.

You can view or update credit card information and designate a different credit card for AWS to charge on the Payment Methods page in the Billing and Cost Management console.

The Billing and Cost Management service provides features you can use to estimate and plan your AWS costs, receive alerts if your costs exceed a threshold that you set, assess your biggest investments in AWS resources, and, if you work with multiple AWS accounts, simplify your accounting.



Here are the main features and capabilities of AWS Billing and Cost Management you should be aware of:

- **Analyzing costs with graphs:** The AWS Billing and Cost Management console includes the Cost Explorer tool for viewing your AWS cost data as a graph. You should note that this valuable tool is provided for you free of charge. With Cost Explorer, you can filter graphs by values such as API operation, Availability Zone, AWS service, custom cost allocation tag, Amazon EC2 instance type, purchase option, region, usage type, usage type group, and more. If you use consolidated billing, you can also filter by member account. In addition, you can see a forecast of future costs based on your historical cost data.
- **Budgets:** You can use budgets to track your AWS usage and costs. Budgets use the cost visualization provided by Cost Explorer to show you the status of your budgets, to provide forecasts of your estimated costs. You can also use Budgets to track your AWS usage, including your Free Tier usage. Finally, you can also use budgets to create Amazon SNS notifications that alert you when you go over your budgeted amounts, or when your estimated costs exceed your budgets.
- **Payment currencies:** You can view your estimated bills and pay your AWS invoices in your preferred currency by setting a payment currency. AWS converts your bill to your preferred currency after your bill is finalized. Until then, all of the preferred currency amounts shown in the console are estimated in USD. AWS guarantees your exchange rate so that refunds use the same exchange rate as your original transaction.

- **AWS Cost and Usage reports:** You can choose to have AWS publish billing reports to an Amazon S3 bucket that you own. You can receive reports that break down your costs by the hour or month, by product or product resource, or by tags that you define yourself. AWS updates the report in your bucket once a day in comma-separated value (CSV) format. You can view the reports using spreadsheet software such as Microsoft Excel or access them from an application using the Amazon S3 API.

EXAM PREPARATION TASKS

As mentioned in the section “How to Use This Book” in the Introduction, you have a few choices for exam preparation: the exercises here, [Chapter 16, “Final Preparation,”](#) and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topics icon in the outer margin of the page. [Table 15-2](#) lists a reference of these key topics and the page numbers on which each is found.



Table 15-2 Key Topics for [Chapter 15](#)

Key Topic Element	Description	Page Number
List	Capabilities of the TCO calculators	
List	Features and capabilities of the AWS Billing and Cost Management service	

Define Key Terms

Define the following key terms from this chapter and check your answers in the Glossary:

TCO calculators

Simple Monthly Calculator

Q&A

The answers to these questions appear in Appendix A. For more practice with exam format questions, use the Pearson Test Prep Software Online.

1. What popular calculator for AWS pre-dated the TCO calculators?
2. Name at least two main features of AWS Billing and Cost Management.

Part V Final Preparation

Chapter 16

Final Preparation

Are you excited for your exam after reading this book? I sure hope so. You should be. In this chapter we put certification prep all together for you. This includes taking a more detailed look at the actual certification exam itself.

This chapter shares some great ideas on ensuring you ace that exam. If you read this book with the interest of really mastering AWS and you were not really considering certification, maybe this chapter will convince you to give it a try!

The first 15 chapters of this book cover the technologies, protocols, design concepts, and considerations required to be prepared to pass the AWS Certified Cloud Practitioner (CLF-C01) exam. Although these chapters supply the detailed information, most people need more preparation than just reading the first 15 chapters of this book. This chapter details a set of tools and a study plan to help you complete your preparation for the exams.

This short chapter has four main sections. The first section lists the AWS Certified Cloud Practitioner exam information and breakdown. The second section shares some important tips to keep in mind to ensure you are ready for this exam. The

third section discusses exam preparation tools useful at this point in the study process. The final section of this chapter lists a suggested study plan now that you have completed all the earlier chapters in this book.

EXAM INFORMATION

Here are details you should be aware of regarding the exam that maps to this text:

Question Types: Multiple choice and multiple choice with multiple correct answers

Number of Questions: 65

Time Limit: 130 minutes

Required Passing Score: 700 out of 1000

Available Languages: English, Japanese, Simplified Chinese, Korean

Exam Fee: 150 USD

Exam ID Code: CLF-C01

This exam seeks to validate the following for a candidate:

- Define what the AWS Cloud is and the basic global infrastructure.
- Describe basic AWS Cloud architectural principles.
- Describe the AWS Cloud value proposition.
- Describe key services on the AWS platform and their common use cases (for example, compute and analytics).

- Describe basic security and compliance aspects of the AWS platform and the shared responsibility security model.
- Define the billing, account management, and pricing models.
- Identify sources of documentation or technical assistance (for example, whitepapers and support tickets).
- Describe basic/core characteristics of deploying and operating in the AWS Cloud.

Amazon Web Service certification exam authors recommend the following skills and experience for candidates wanting to pass this exam:

- Have at least 6 months of experience with the AWS Cloud in any role, including technical, managerial, sales, purchasing, or financial. Candidates should have a basic understanding of IT services and their uses in the AWS Cloud platform.

The exam is broken up into four different domains. Here are those domains and the percentage of the exam for each:

- **Cloud Concepts:** 28 percent
- **Security:** 24 percent
- **Technology:** 36 percent
- **Billing and Pricing:** 12 percent

Here is the breakdown of the exact exam objectives for these various domains:

Domain 1: Cloud Concepts

- 1.1 Define the AWS Cloud and its value proposition
- 1.2 Identify aspects of AWS Cloud economics
- 1.3 List the different cloud architecture design principles

Domain 2: Security

- 2.1 Define the AWS Shared Responsibility model
- 2.2 Define AWS Cloud security and compliance concepts
- 2.3 Identify AWS access management capabilities
- 2.4 Identify resources for security support

Domain 3: Technology

- 3.1 Define methods of deploying and operating in the AWS Cloud
- 3.2 Define the AWS global infrastructure
- 3.3 Identify the core AWS services
- 3.4 Identify resources for technology support

Domain 4: Billing and Pricing

- 4.1 Compare and contrast the various pricing models for AWS

4.2 Recognize the various account structures in relation to AWS billing and pricing

4.3 Identify resources available for billing support

GETTING READY

Here are some important tips to keep in mind to ensure you are ready for this rewarding exam!

- **Build and use a study tracker:** Consider taking the exam objectives shown in this chapter and build yourself a study tracker! This will help ensure you have not missed anything and that you are confident for your exam! As a matter of fact, this book offers a sample Study Planner as a website supplement.
- **Think about your time budget for questions in the exam:** When you do the math, you realize that you have 2 minutes per question. Although this does not sound like enough time, realize that many of the questions will be very straightforward, and you will take 15 to 30 seconds on those. This builds time for other questions as you take your exam.
- **Watch the clock:** Check in on the time remaining periodically as you are taking the exam. You might even find that you can slow down pretty dramatically as you have built up a nice block of extra time.
- **Get some ear plugs:** The testing center might provide ear plugs, but get some just in case and bring them along. There might be other test takers in the center with you, and

you do not want to be distracted by their screams. I personally have no issue blocking out the sounds around me, so I never worry about this, but I know it is an issue for some.

- **Plan your travel time:** Give yourself extra time to find the center and get checked in. Be sure to arrive early. As you test more at that center, you can certainly start cutting it closer time-wise.
- **Get rest:** Most students report success with getting plenty of rest the night before the exam. All-night cram sessions are not typically successful.
- **Bring in valuables but get ready to lock them up:** The testing center will take your phone, your smart watch, your wallet, and other such items. It will provide a secure place for them.
- **Take notes:** You will be given note-taking implements, so do not be afraid to use them. For example, I always end up jotting down any questions I struggled with. I then memorize these at the end of the test by reading my notes over and over again. I then always make sure I have a pen and paper in the car. I write down the issues in there just after the exam. When I get home with a pass or fail, I research those items!
- **Use the FAQs in your study:** The Amazon test authors have told me they love to pull questions from the FAQs they publish at the AWS site. These are a really fun and valuable read anyway, so go through them for the various services that are key for this exam.

- **Practice exam questions are great—use them:** This text provides many practice exam questions. Be sure to go through them thoroughly. Remember, just don't blindly memorize answers; let the questions really demonstrate where you are weak in your knowledge and then study up on those areas.

TOOLS FOR FINAL PREPARATION

This section lists some information about the available tools and how to access them.

Pearson Cert Practice Test Engine and Questions on the Website

Register this book to get access to the Pearson IT Certification test engine (software that displays and grades a set of exam-realistic multiple-choice questions). Using the Pearson Cert Practice Test Engine, you can either study by going through the questions in Study mode or take a simulated (timed) AWS Certified Cloud Practitioner exam.

The Pearson Test Prep practice test software comes with two full practice exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep software.

Accessing the Pearson Test Prep Software Online

The online version of this software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, follow these steps:

Step 1. Go to <http://www.PearsonTestPrep.com>.

Step 2. Select **Pearson IT Certification** as your product group.

Step 3. Enter your email/password for your account. If you don't have an account on PearsonITCertification.com or CiscoPress.com, you will need to establish one by going to PearsonITCertification.com/join.

Step 4. In the **My Products** tab, click the **Activate New Product** button.

Step 5. Enter the access code printed on the insert card in the back of your book to activate your product.

Step 6. The product will now be listed in your My Products page. Click the **Exams** button to launch the exam settings screen and start your exam.

Accessing the Pearson Test Prep Software Offline

If you want to study offline, you can download and install the Windows version of the Pearson Test Prep software. You can find a download link for this software on the book's companion website, or you can just enter this link in your browser:

<http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip>

To access the book's companion website and the software, follow these steps:

- Step 1.** Register your book by going to PearsonITCertification.com/register and entering the ISBN: 9780789760487.
- Step 2.** Respond to the challenge questions.
- Step 3.** Go to your account page and select the **Registered Products** tab.
- Step 4.** Click the **Access Bonus Content** link under the product listing.
- Step 5.** Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
- Step 6.** After the software finishes downloading, unzip all the files on your computer.
- Step 7.** Double-click the application file to start the installation and follow the on-screen instructions to complete the registration.
- Step 8.** After the installation is complete, launch the application and select the **Activate Exam** button on the My Products tab.
- Step 9.** Click the **Activate a Product** button in the Activate Product Wizard.
- Step 10.** Enter the unique access code found on the card in the back of your book and click the **Activate** button.

Step 11. Click **Next** and then the **Finish** button to download the exam data to your application.

Step 12. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

The offline and online versions will synch together, so saved exams and grade results recorded on one version will also be available to you on the other.

Customizing Your Exams

When you are in the exam settings screen, you can choose to take exams in one of three modes:

- Study mode
- Practice Exam mode
- Flash Card mode

Study mode allows you to fully customize your exams and review answers as you are taking an exam. This is typically the mode you would use first to assess your knowledge and identify information gaps. Practice Exam mode locks certain customization options because it is presenting a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the

detailed score reports that the other two modes do, so you should not use it if you are trying to identify knowledge gaps.

In addition to these three modes, you are able to select the source of your questions. You can choose to take exams that cover all the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you want to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you as well as two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

You can make several other customizations to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if any updates are available for your exam data and automatically download any changes that were made since the last time you used the software. This requires that you are connected to the Internet at the time you launch the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the **Tools** tab and select the **Update Products** button. Again, this is only an issue with the Windows desktop application.

If you want to check for updates to the Pearson Test Prep exam engine software, Windows desktop version, simply select the **Tools** tab and select the **Update Application** button. This way, you ensure you are running the latest version of the software engine.

Premium Edition

In addition to the free practice exam provided on the website, you can purchase additional exams with expanded functionality directly from Pearson IT Certification. The Premium Edition of this title contains an additional two full

practice exams and an eBook (in both PDF and ePub format). In addition, the Premium Edition title also has remediation for each question to the specific part of the eBook that relates to that question.

Because you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. A coupon code in the book sleeve contains a one-time-use code and instructions for where you can purchase the Premium Edition.

To view the Premium Edition product page, go to www.informit.com/title/9780789760487.

Chapter-Ending Review Tools

Chapters 1 through 15 have several features in the “Exam Preparation Tasks” and “Q&A” sections at the end of the chapter. You might have already worked through these in each chapter. Using these tools again can also be useful as you make your final preparations for the exam.

SUGGESTED PLAN FOR FINAL REVIEW/STUDY

This section lists a suggested study plan from the point at which you finish reading through Chapter 15 until you take the AWS Certified Cloud Practitioner exam. Certainly, you can ignore this plan, use it as is, or just take suggestions from it.

The plan uses these steps:

Step 1. Review key topics and “DIKTA?” questions: You can use the table that lists the key topics in each chapter or just flip the pages looking for key topics. Also, reviewing the “DIKTA?” questions from the beginning of the chapter can be helpful for review.

Step 2. Review “Q&A” sections: Go through the Q&A questions at the end of each chapter to identify areas where you need more study.

Step 4. Use the Pearson Cert Practice Test engine to practice: You can use the Pearson Cert Practice Test engine to study using a bank of unique exam-realistic questions available only with this book.

SUMMARY

The tools and suggestions listed in this chapter have been designed with one goal in mind: to help you develop the skills required to pass the AWS Certified Cloud Practitioner exam. This book has been developed from the beginning to not only tell you the facts but also to help you learn how to apply the facts. No matter what your experience level leading up to taking the exams, it is our hope that the broad range of preparation tools, and even the structure of the book, helps you pass the exam with ease. We hope you do well on the exam.

Part VI Appendixes

Glossary of Key Terms

Agility The ability of AWS to foster innovation in organizations.

API An application programming interface provides programmatic access to resources in AWS.

API Gateway A fully managed service that allows you to create and publish secure APIs to scale in AWS.

Artifact A central resource for compliance-related information.

Auto Scaling The automatic addition and subtraction of resources based on various factors, often the demand for the resources.

Automation The automatic generation and/or performance of required IT tasks.

Availability Ensuring data is available when needed.

Availability Zone A division of geographic locations within regions; each Availability Zone contains at least one separate and distinct data center.

AWS Auditor Learning Path A Learning Path for AWS that focuses on those in auditor, compliance, and legal roles.

AWS Global Infrastructure The resources owned by AWS around the globe and used by customers.

AWS Partner Network The AWS global partner program that seeks to help partners build successful AWS solutions.

AWS Professional Services An organization that is made up of a global team of experts that can help you with your desired business outcomes for AWS.

Basic support plan The AWS support plan that is included free of charge for every account.

Business support plan The third tier of four tiers of support plans; this plan features a response time to your issues of 1 hour.

CapEx Capital expenditures.

ClassicLink Allows the linking of EC2-Classic instances to a VPC in your account.

CloudFormation Gives developers and systems administrators an easy way to create and manage a collection of related AWS resources, provisioning and updating them in an orderly and predictable fashion.

CloudFront A global content delivery network (CDN) service that accelerates delivery of your websites, APIs, video content, or other web assets.

CloudTrail A web service that records AWS API calls for your account and delivers log files to you.

CloudWatch A monitoring service for AWS Cloud resources and the applications you run on AWS.

CodeDeploy A fully managed code deployment service that helps you deploy software to things like EC2 instances.

Community cloud A cloud provisioned for use by a select group of companies or organizations.

Compliance Conformity in fulfilling specific requirements.

Confidentiality Keeping data secure (often through encryption).

Developer support plan The second possible tier of the four tiers of support; this is the first level of support plan that provides you with access to tech support.

Direct Connect An alternative to a shared Internet connection to AWS; Direct Connect is a completely private connection from your on-premises network to the AWS facilities.

DynamoDB A fast and flexible NoSQL database service for all applications that need consistent, single-digit millisecond latency at any scale.

EBS Elastic Block Store offers persistent block storage volumes for use with EC2 instances.

EC2 Elastic Compute Cloud makes virtual machines available in AWS and provides a managed environment for your Docker containers.

Edge Locations Locations that deliver cached CloudFront content.

EFS The Elastic File System provides simple, scalable file storage for use with Amazon EC2 instances in the AWS Cloud.

Elastic Beanstalk A service that permits you to upload your code and have it hosted automatically by AWS.

Elastic Load Balancing The AWS tool for distributing requests for a resource among various resources.

ElastiCache A web service that makes it easy to deploy, operate, and scale an in-memory cache in the cloud.

Elasticity The ability of the cloud to grow or shrink resources dynamically based on demand or other factors.

Enterprise support plan The premier level of support available in AWS; this plan features a response time of just 15 minutes to major issues you are experiencing.

Federation Permitting an account to use its access with another trusted service in order to access AWS.

Free Tier A trial account for AWS that is completely free, given certain constraints.

FT Fault tolerance. The property that enables a system to continue operating properly in the event of the failure of some (one or more faults within) of its components.

Glacier A secure, durable, and extremely low-cost storage service for data archiving and long-term backup.

Groups A collection of user accounts; permissions are assigned to groups.

HA High availability. A characteristic of a system that aims to ensure an agreed level of operational performance, usually uptime, for a higher than normal period.

Hybrid cloud Companies that host some cloud technologies privately and rely on public cloud resources for other technologies.

IaaS Infrastructure as a Service.

IAM Identity and Access Management enables you to securely control access to AWS services and resources for your users.

Integrity Ensuring data is not manipulated at rest or in transit.

Lambda The main serverless compute service of AWS.

MFA Multi-factor authentication.

Network ACLs Used to control traffic moving between subnets in your VPC.

Networking and Content Delivery A service category that features low-latency delivery of cached content to specific geographic locations.

On-demand instances EC2 instances that are launched at a current price of compute time.

OpEx Operational expenditures.

OpsWorks A configuration management service that uses Chef or Puppet, an automation platform that treats server configurations as code.

Orchestration The scheduling and coordination of automated tasks for an entire process or workflow.

PaaS Platform as a Service.

Private cloud Cloud technology kept “in-house” and fully managed by the private organization.

Public cloud Massive cloud providers that make various “as a Service” models available to the public.

RDS Relational Database Services makes it easy to set up, operate, and scale a relational database in the cloud.

Redshift A fast, fully managed, petabyte-scale data warehouse that makes it simple and cost-effective to analyze all your data using your existing business intelligence tools.

Region A physical, geographic location in the world where AWS creates multiple Availability Zones.

Reserved instances Instances at a fixed price that you have contractually reserved for your purposes.

Roles Similar to user accounts but with no credentials; used to provide access from one AWS service to another.

Route 53 A highly available and scalable cloud Domain Name System (DNS) web service.

S3 The Simple Storage Service of AWS is flexible, object-based storage for a wide variety of purposes.

SaaS Software as a Service.

Security groups Built-in firewalls that are associated with EC2 instances and provide security at the protocol and port level.

Security in the cloud The reference to the client security responsibilities in the AWS Shared Responsibility model.

Security of the cloud The reference to the Amazon security responsibilities in the AWS Shared Responsibility model.

Service Catalog Allows you to create and maintain a catalog of IT resources approved for use with AWS.

Simple Monthly Calculator A free AWS tool that allows you to calculate your monthly AWS costs for various services.

Spot instances Instances where you bid on unused capacity in AWS.

Systems Manager A tool for grouping your resources for ease of monitoring and configuration changes.

AWS Shared Responsibility model The overall security model followed by AWS; this model divides the client responsibilities from those of Amazon.

Total Cost of Ownership calculators A set of free AWS tools that permit you to reduce TCO by estimating cost savings using AWS.

Trusted Advisor A management tool that checks your configurations and provides modification advice to help you adhere to best practices.

Users Entities created to represent individuals who need access to AWS.

VPC The Virtual Private Cloud that provides the virtual network components in AWS.

VPC endpoint Permits private connections from your VPC to supported AWS services.

VPC peering A connection between multiple VPCs in AWS.

Whitepapers Documents made available by Amazon that provide valuable best practices and architectures to follow.

Appendix A

Answers to the “Do I Know This Already?” Quizzes and Q&A Sections

DO I KNOW THIS ALREADY? ANSWERS

Chapter 1

1. d

2. c

3. b

4. b

5. a

6. d

Chapter 2

1. d

2. b

3. b

4. a

5. b

6. d

Chapter 3

1. c

2. b

3. b

4. a

5. d

6. a and d

7. c

8. d

9. c

10. b

11. c

12. d

13. a

14. d

15. a

Chapter 4

1. d

2. d

3. a

4. d

5. b

6. c

Chapter 5

1. a and d

2. c

3. b

4. d

5. c

Chapter 6

1. c

2. b

3. b and c

4. d

Chapter 7

1. d

2. b

3. a

4. c

Chapter 8

1. c

2. a

3. d

4. d

Chapter 9

1. d

2. a

3. c

4. b

5. d

6. b

Chapter 10

1. a

2. d

3. a

4. a

5. c

6. a

7. a

8. b

9. b

Chapter 11

1. c

2. a

3. b

4. a

Chapter 12

1. b

2. c

3. a

4. c

Chapter 13

1. d

2. b

3. a

4. c

Chapter 14

1. d

2. c

3. b and c

4. c

Chapter 15

1. a and d

2. c

3. a

4. a

Q&A ANSWERS

Chapter 1

1. On-demand self-service

Broad network access

Resource pooling

Rapid elasticity

Measured service

2. IaaS

PaaS

SaaS

3. Private

Public

Hybrid

Community

4. Lambda
5. Elastic Block Store (EBS)
6. CloudTrail

Chapter 2

1. You determine which region these resources exist in.
2. API calls.
3. In geographically distant parts of AWS regions. These are located all around the world.

Chapter 3

1. On-demand, reserved, and spot
2. Regions, Availability Zones (AZs), and Edge Locations
3. MySQL and PostgreSQL

Chapter 4

1. Operational excellence
 - Security
 - Reliability
 - Performance efficiency
 - Cost optimization
2. Fault tolerance (FT) is often considered a subcomponent of HA.
3. EC2

Chapter 5

1. The physical and environmental security controls used by Amazon

2. Customer data

Platform, applications, Identity and Access Management (IAM) policies

Guest operating systems

Network and firewall configurations

Client-side data encryption

Server-side encryption (file system and or data)

Networking traffic protection (encryption, integrity, and identity)

3. Cloud software, including compute, storage, networking, and database software

Hardware

AWS Global Infrastructure, including regions, Availability Zones, and Edge Locations

Chapter 6

1. The AWS Marketplace offers many affordable (and free) security solutions. These might include anti-malware, IPS, and policy management tools.

2. You must contact AWS support personnel. You are not permitted to penetration test your data and resources

without the explicit permission and knowledge of AWS staff.

Chapter 7

1. Roles
2. The root account

Chapter 8

1. Possible answers include CJIS, FedRAMP TIC, FISC, FISMA, GxP (FDA 21 CFR Part 11), IT-Grundschutz, MPAA, NERC, NIST, and UK Cyber Essentials.
2. Enterprise

Chapter 9

1. Backup generation and retention
 - Security compliance
 - Code deployments
 - AWS infrastructure changes
2. The AWS Management Console
 - The AWS CLI
 - SDKs and APIs

Chapter 10

1. The AWS Global Infrastructure features regions with Availability Zones inside of them. Each Availability Zone

- features at least one discrete data center.
- 2. Amazon ensures that the Availability Zones are as far apart as possible to promote fault tolerance and disaster recovery. Separate flood plains are targeted.
- 3. VPC peerings permit inter-VPC communications.

Chapter 11

- 1. User guides
 - API references
 - CLI references
- 2. At least a Free Tier account with AWS

Chapter 12

- 1. Possible answers include NS, SQS, CloudWatch, Lambda, and Key Management Service.
- 2. In order to remain within the Free Tier limits.

Chapter 13

- 1. Compute, Storage, and Data Transfer Out (aggregated across services)
- 2. Storage class, requests, and data transfer out

Chapter 14

- 1. Proactive guidance, best practices, account assistance, and launch support

2. Basic, Developer, Business, and Enterprise

Chapter 15

1. The AWS Simple Monthly Calculator

2. Analyzing costs with graphs

Budgets

Payment currencies

AWS Cost and Usage reports

Appendix B

AWS Certified Cloud Practitioner (CLF-C01) Cert Guide Exam Updates

Over time, reader feedback allows Pearson to gauge which topics give our readers the most problems when taking the exams. To assist readers with those topics, the authors create new materials clarifying and expanding on those troublesome exam topics. As mentioned in the Introduction, the additional content about the exam is contained in a PDF on this book's companion website, at <http://www.ciscopress.com/title/9780789760487>.

This appendix is intended to provide you with updated information if Amazon makes minor modifications to the exam upon which this book is based. When Amazon releases an entirely new exam, the changes are usually too extensive to provide in a simple update appendix. In those cases, you might need to consult the new edition of the book for the updated content. This appendix attempts to fill the void that occurs with any print book. In particular, this appendix does the following:

- Mentions technical items that might not have been mentioned elsewhere in the book

- Covers new topics if Amazon adds new content to the exam over time
- Provides a way to get up-to-the-minute information about content for the exam

ALWAYS GET THE LATEST AT THE BOOK'S PRODUCT PAGE

You are reading the version of this appendix that was available when your book was printed. However, given that the main purpose of this appendix is to be a living, changing document, it is important that you look for the latest version online at the book's companion website. To do so, follow these steps:

Step 1. Browse to www.ciscopress.com/title/9780789760487.

Step 2. Click the **Updates** tab.

Step 3. If there is a new [Appendix B](#) document on the page, download the latest Appendix B document.

NOTE

The downloaded document has a version number. Comparing the version of the print [Appendix B](#) (version 1.0) with the latest online version of this appendix, you should do the following:

- **Same version:** Ignore the PDF that you downloaded from the companion website.
- **Website has a later version:** Ignore this [Appendix B](#) in your book and read only the latest version that you downloaded from the companion website.

TECHNICAL CONTENT

The current version (1.0) of this appendix does not contain additional technical coverage.

Appendix C Study Planner

[This content is currently in development.]

This content is currently in development.