PEARSON IT CERTIFICATION

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

AWS Certified Solutions Architect – Associate

(SAA-C03)

MARK WILKINS

FREE SAMPLE CHAPTER |

AWS Certified Solutions Architect – Associate (SAA-C03) Cert Guide

Access interactive study tools on this book's companion website, including practice test software, review questions, Key Term flash card application, a study planner, and more!

To access the companion website, simply follow these steps:

1. Go to **www.pearsonITcertification.com/register**.
2. Enter the print book ISBN: **9780137941582**.
3. Answer the security question to validate your purchase.
4. Go to your account page.
5. Click on the **Registered Products** tab.
6. Under the book listing, click on the Access Bonus Content link.

If you have any issues accessing the companion website, you can contact our support team by going to **http://pearsonitp.echelp.org.**

Pearson Test Prep online system requirements:
Browsers: Chrome version 73 and above; Safari version 12 and above; Microsoft Edge 44 and above.
Devices: Desktop and laptop computers, tablets running Android v8.0 and above or iPadOS v13 and above, smartphones running Android v8.0 and above or iOS v13 and above with a minimum screen size of 4.7". Internet access required.

Pearson Test Prep offline system requirements:
Windows 10, Windows 8.1; Microsoft .NET Framework 4.5 Client; Pentium-class 1 GHz processor (or equivalent); 512 MB RAM; 650 MB disk space plus 50 MB for each downloaded practice exam; access to the Internet to register and download exam databases.

AWS Certified Solutions Architect – Associate (SAA-C03) Cert Guide

Mark Wilkins

Pearson

AWS Certified Solutions Architect – Associate (SAA-C03) Cert Guide

ISBN-13: 978-0-13-794158-2

ISBN-10: 0-13-794158-7

Library of Congress Control Number: 2023930964

ScoutAutomatedPrintCode

Vice President, IT Professional
Mark Taub

Director, ITP Product Management
Brett Bartow

Executive Editor
Nancy Davis

Development Editor
Christopher Cleveland

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Bill McManus

Indexer
Jen Hinchliffe

Proofreader
Jen Hinchliffe

Technical Editor
Ralph Parisi

Publishing Coordinator
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where

- Everyone has an equitable and lifelong opportunity to succeed through learning
- Our educational products and services are inclusive and represent the rich diversity of learners
- Our educational content accurately reflects the histories and experiences of the learners we serve
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview)

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

This page intentionally left blank

Contents at a Glance

Table of Contents

About the Author

Mark Wilkins is an electronics engineering technologist with a wealth of experience in designing, deploying, and supporting software and hardware technology in the corporate and small business world. Since 2013, Mark has focused on supporting and designing cloud service solutions with Amazon Web Services, Microsoft Azure, and the IBM Cloud. He is certified as an AWS Certified Solutions Architect – Associate. Mark is also a Microsoft Certified Trainer (MCT) and holds certifications in MCTS, MCSA, Server Virtualization with Windows Server Hyper-V, and Azure Cloud Services.

Mark worked as a technical evangelist for IBM SoftLayer from 2013 through 2016 and taught both SoftLayer fundamentals and SoftLayer design classes to many Fortune 500 companies in Canada, the United States, Europe, and Australia. As former course director for Global Knowledge, Mark developed and taught many technical seminars, including Configuring Active Directory Services, Configuring Group Policy, and Cloud and Virtualization Essentials. Mark currently develops AWS curriculum on AWS cloud services and certification for O'Reilly Media and LinkedIn Learning. To learn more about what Mark finds interesting about the cloud, visit The Cloud Thingy, at https://thecloudthingy.substack.com/. To learn more about the AWS cloud and AWS certification, check out Mark's YouTube channel at http://www.youtube.com/@SAA-C03.

Mark's published books include *Windows 2003 Registry for Dummies*, *Administering SMS 3.0*, *Administering Active Directory*, and *Learning Amazon Web Services (AWS): A Hands-On Guide to the Fundamentals of AWS Cloud*.

Dedication

I would like to dedicate this book to my grandson, Silas, a future nerd. And to Bruce, one of our cats, for making me take breaks when he wanted.

Acknowledgments

This manuscript was made truly great by the incredible project management of Tonya Simpson, who went above and beyond! Thanks so much.

I would also like to express my gratitude to Chris Cleveland, the development editor of this book. I was lucky to work with him on this text. Chris helped make this book several cuts above the rest.

Finally, thanks so much to Nancy Davis, my tireless acquisitions editor. Nancy very patiently made this book a reality.

About the Technical Reviewer

Ralph Parisi is a certified Champion Authorized Amazon instructor and has been teaching AWS courses for 6 years. Ralph has been an instructor for more than 20 years and has taught technical classes for Microsoft Exchange Server, Microsoft Windows Server, Active Directory, Group Policy, Citrix XenDeskop, and XenApp. Ralph has worked as a consultant to large corporations architecting Exchange Server and Active Directory solutions and migrations. Ralph has also worked with various companies as a technical writer. Ralph lives in North Carolina with his wife and Saluki, Dillon.

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 Solutions Architect – Associate (SAA-C03) 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 9780137941582 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

There are many reasons to get certified in AWS technology. First of all, AWS certifications validate your AWS cloud knowledge. To fully understand the AWS cloud, preparing for the AWS Certified Solutions Architect – Associate (SAA-C03) exam is a great place to start. There are other AWS certifications that may be a better fit, depending on your technical level, your current knowledge of cloud concepts, and your current and future jobs with AWS technologies and services. Certifications are broken down into Foundational, Associate, Professional, and Specialty certifications. Full details can be found at https://aws.amazon.com/certification/. AWS frequently adds new certification tracks, but the following are the certifications that are currently available:

- **Foundational:** There is one Foundational certification: AWS Certified Cloud Practitioner. The recommendation is to have at least 6 months of fundamental AWS cloud knowledge before attempting this certification exam. You might be closer to this certification than you think, depending on your current level of technical skills. One advantage of taking the AWS Certified Cloud Practitioner exam first is that it helps you to get used to answering multiple-choice test questions and to learn about the foundational AWS cloud services.
- **Associate:** There are several Associate certifications:
  - **AWS Certified Solutions Architect – Associate:** For individuals working as solutions architects, designing AWS solutions using AWS services
  - **AWS Certified SysOps Administrator – Associate:** For individuals working as systems administrators, managing and operating AWS services
  - **AWS Certified Developer – Associate:** For individuals working as developers, deploying and debugging cloud-based applications hosted at AWS

    Each certification exam expects that you know how the AWS service that you are being tested on works. Each Associate certification has a specific focus:
  - **Architect:** The best design possible, based on the question and scenario
  - **SysOps:** The administration steps required to carry out a particular task
  - **Developer:** How to best use the service for the hosted application you are writing

For example, the three Associate exams would test different aspects of CloudWatch logs:

- **Architect:** The main focus of this exam is on how CloudWatch logs work and the main design features to consider based on specific needs—that is, design knowledge related to using CloudWatch logs for a variety of solutions.
- **SysOps:** The main focus of this exam is on how to configure CloudWatch logs based on specific needs—that is, configuration and deployment of CloudWatch logs using operational knowledge.
- **Developer:** The main focus of this exam is on what CloudWatch logs are useful for when developing applications for tracking performance of an application hosted on an EC2 instance—that is, knowledge of how a particular AWS service can help in the development and testing process with applications.

  Before you attempt one of the Associate certifications, AWS recommends that you have at least 1 year of experience solving problems and implementing solutions using AWS services. AWS really wants to ensure that you have hands-on experience solving problems.

- **Professional:** These certifications include the AWS Certified Solutions Architect Professional and the AWS Certified DevOps Engineer Professional. Professional certifications are not where you normally start your certification journey. AWS recommends that you have at least 2 years of hands-on experience before taking a Professional exam.
- **Specialty:** The Specialty certifications for Advanced Networking, Security, Machine Learning, Data Analytics, SAP on AWS, and Database require advanced knowledge of the subject matter. AWS recommends that you have an Associate certification before you attempt one of these certifications.

NOTE The AWS Certified Solutions Architect – Associate (SAA-C03) certification is globally recognized and does an excellent job of demonstrating that the holder has knowledge and skills across a broad range of AWS topics.

The Goals of the AWS Certified Solutions Architect – Associate Certification

The AWS Certified Solutions Architect – Associate certification is intended for individuals who perform in a solutions architect role. This exam validates a candidate's ability to effectively demonstrate knowledge of how to architect and deploy secure and robust applications on AWS technologies. It validates a candidate's ability to

- Have knowledge and skills in the following AWS services: compute, networking, storage, and database and deployment and management services

- Have knowledge and skills in deploying, managing, and operating AWS workloads and implementing security controls and compliance requirements
- Identify which AWS service meets technical requirements
- Define technical requirements for AWS-based applications
- Identify which AWS services meet a given technical requirement

Recommended Prerequisite Skills

While this book provides you with the information required to pass the Certified Solutions Architect – Associate (SAA-C03) exam, Amazon considers ideal candidates to be those who possess the following:

- Experience in AWS technology
- Strong on-premises IT experience
- Understanding of mapping on-premises technology to the cloud
- Experience with other cloud services

The Exam Domains

The AWS Certified Solutions Architect – Associate (SAA-C03) exam is broken down into four major domains. This book covers each of the domains and the task statements.

- **Domain 1: Design Secure Architectures 30%**
  - Task Statement 1: Design secure access to AWS resources
  - Task Statement 2: Design secure workloads and applications
  - Task Statement 3: Determine appropriate data security controls
- **Domain 2: Design Resilient Architectures 26%**
  - Task Statement 1: Design scalable and loosely coupled architectures
  - Task Statement 2: Design highly available and/or fault-tolerant architectures
- **Domain 3: Design High-Performing Architectures 24%**
  - Task Statement 1: Determine high-performing and/or scalable storage solutions
  - Task Statement 2: Design high-performing and elastic compute solutions
  - Task Statement 3: Determine high-performing database solutions

- Task Statement 4: Determine high-performing and/or scalable network architectures
- Task Statement 5: Determine high-performing data ingestion and transformation solutions

- **Domain 4: Design Cost-Optimized Architectures 20%**
  - Task Statement 1: Design cost-optimized storage solutions
  - Task Statement 2: Design cost-optimized compute solutions
  - Task Statement 3: Design cost-optimized database solutions
  - Task Statement 4: Design cost-optimized network architectures

Steps to Becoming an AWS Certified Solutions Architect – Associate

To become an AWS Certified Solutions Architect – Associate, an exam candidate must meet certain prerequisites and follow specific procedures. Exam candidates must ensure that they have the necessary background and technical experience for the exam and then sign up for the exam.

Signing Up for the Exam

The steps required to sign up for the AWS Certified Solutions Architect – Associate exam are as follows:

Step 1. Create an AWS Certification account at https://www.aws.training/Certification and schedule your exam from the home page by clicking Schedule New Exam.

Step 2. Select a testing provider, either Pearson VUE or PSI, and select whether you want to take the exam at a local testing center or online from your home or office. If you choose to take an online exam, you will have to agree to the online testing policies.

Step 3. Complete the examination signup by selecting the preferred language and the date of your exam.

Step 4. Submit the examination fee.

TIP Refer to the AWS Certification site at https://aws.amazon.com/certification/ for more information regarding this and other AWS certifications.

How to Use This Book

This book maps directly to the domains of the AWS Certified Solutions Architect – Associate (SAA-C03) exam and includes a number of features that 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 ensure 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 truly learn and understand the topics. This book is designed to help you pass the AWS Certified Solutions Architect – Associate (SAA-C03) 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:** The sections under "Foundation Topics" describe the core topics of each chapter.
- **Exam Preparation Tasks:** The "Exam Preparation Tasks" section lists a series of study activities that you should do at the end of each 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 the number of the page where you can find more information about each one. Although the contents of the entire chapter could be tested on the exam, you should definitely know the information listed in each key topic, so you should review these.
  - **Define Key Terms:** Although the AWS Certified Solutions Architect – Associate (SAA-C03) exam may be unlikely to word a question "Define

this term," the exam does require that you learn and know a lot of terminology. This section lists the most important terms from the chapter and asks you to write a short definition and compare your answer to the glossary at the end of the book.

- **Q&A:** Confirm that you understand the content that you just covered by answering these questions and reading the answer explanations.

- **Web-based practice exam:** The companion website includes the Pearson Test Prep practice test engine, which enables 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 14 core chapters—Chapters 2 through 15. Chapter 1 introduces the foundations of AWS, and Chapter 16 provides preparation tips and suggestions for how to approach the exam. Each core chapter covers a specific task statement or multiple task statements of the domains for the AWS Certified Solutions Architect – Associate (SAA-C03) exam.

Companion Website

Register this book to get access to the Pearson Test Prep practice test software and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exam. Be sure to check the box indicating 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 https://www.pearsonitcertification.com/register and log in or create a new account.

Step 2. Enter the ISBN 9780137941582.

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 these steps, please visit https://www.pearsonITcertification.com/contact and select the Site Problems/ Comments option from the Select a Topic drop-down list. Our customer service representatives will assist you.

Pearson Test Prep Practice Test Software

As noted earlier, the Pearson Test Prep practice test software comes with two full practice exams. These practice exams 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 at the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep practice test software. For more information about the practice exams and more tools for exam preparation, see Chapter 16.

Figure Credits

Cover: Yurchanka Siarhei/Shutterstock

Chapter opener: Charlie Edwards/Getty Images

Figures 1.1, 1.3 through 1.6, 1.10, 1.12 through 1.4, 2.1 through 2.4, 2.6 through 2.8, 2.13, 2.14, 3.1 through 3.4, 3.7 through 3.9, 3.11 through 3.24, 3.27 through 3.37, 3.39 through 3.48, 4.3, 4.4, 4.6 through 4.8, 4.11 through 4.14, 4.22 through 4.34, 5.2, 5.6 through 5.11, 5.14 through 5.16, 5.18, 6.7, 6.11 through 6.15, 6.17 through 6.20, 6.22, 6.23, 6.26 through 6.30, 7.5, 7.11 through 7.14, 7.33, 7.34, 8.1 through 8.13, 8.15, 8.17 through 8.23, 9.2 through 9.5, 9.7, 9.9, 9.10, 9.12, 9.13 through 9.29, 10.1, 10.4, 10.10 through 10.12, 10.17, 10.18, 11.3 through 11.7, 11.10 through 11.21, 11.23, 11.24, 11.27 through 11.31, 11.33, 11.34, 12.1 through 12.10, 12.12 through 12.17, 13.3 through 13.12, 14.1, 14.3 through 14.6, 14.13, 15.4, 16.1, 16.2: Amazon Web Services, Inc

Figure 2.11: Adam Wiggins

Figures 2.9a, 7.1: Andrei Minsk/Shutterstock

Figures 3.10, 3.38, 11.25: Microsoft Corporation

This page intentionally left blank

Determining Appropriate Data Security Controls

Organizations have workloads and associated cloud services fail while operating at AWS. Amazon Elastic Compute Cloud (EC2) instances fail, Amazon Elastic Block Store (EBS) volumes crash, and cloud services can stop working. However, you shouldn't have go to your boss and announce, "We've lost some data." Fortunately, all data can be securely and redundantly stored at AWS.

All data stored at AWS using any storage service can be encrypted; organizations make the decision about whether encryption is required. However, Amazon S3 objects and S3 Glacier archive storage *is* automatically encrypted at rest. All other storage services at AWS store data records in an unencrypted state to start. For example, Amazon S3 buckets are encrypted using server-side encryption using Amazon S3, the AWS Key Management Service (KMS) with customer master keys (CMK) and data keys, or encryption keys supplied by each organization. Amazon EBS volumes—both boot and data volumes—can be encrypted at rest and in transit using CMKs provided by AWS KMS. Shared storage services such as Amazon EFS and Amazon FSx for Windows File Server can also be encrypted at rest, as can Amazon DynamoDB tables, Amazon Relational Database Service (RDS) deployments, and Amazon Simple Queue Service (SQS) queues.

NOTE Use of master/slave terms in the following chapter is ONLY in association with the official terminology used in industry specifications and/or standards, and in no way diminishes Pearson's commitment to promoting diversity, equity, and inclusion, and challenging, countering, and/or combating bias and stereotyping in the global population of the learners we serve.

AWS does not have single-tenant persistent data storage for individual organizations; all storage services offered at AWS are multi-tenant by design. AWS has the responsibility to ensure that each organization's stored data records are isolated to the AWS account in which they are first created. Organizations can secure data at rest by choosing to encrypt all data records; protecting data in transit can be achieved using Transport Layer Security (TLS).

Each organization is in control of the storage and retrieval of its data records that are stored at AWS. It's the organization's responsibility to define the security and accessibility of all data records stored at AWS. All data storage at AWS starts as private storage only accessible across the AWS private network. Organizations can choose to make select Amazon S3 buckets public, but all other storage services offered by AWS remain private and are not publicly accessible across the Internet. AWS VPN and AWS Direct Connect connections from on-premises locations can directly access AWS storage services; however, EBS volumes can only be accessed through the attached EC2 instance. Figure 5-1 illustrates the options for data encryption at AWS that are discussed in this chapter.

Key Topic

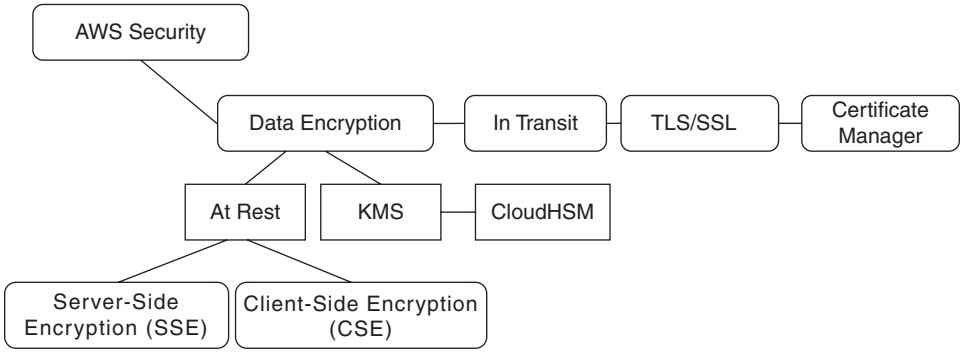

Figure 5-1 Encryption Choices at AWS

"Do I Know This Already?"

The "Do I Know This Already?" quiz allows you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 5-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Q&A Sections."

Table 5-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Data Access and Governance	1, 2
Amazon EBS Encryption	3, 4
Amazon S3 Bucket Security	5, 6
AWS Key Management Service	7, 8
AWS Certificate Manager	9, 10

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 AWS service assists in protecting access to AWS?
    a. AWS Shield
    b. Amazon Macie
    c. Amazon EBS volumes
    d. Amazon DynamoDB databases

2. What is the purpose of using detective controls?
    a. To enable and enforce multifactor access
    b. To detect and alert when security controls change
    c. To manage AWS Organizations backups
    d. To analyze compliance levels

3. Which of the following determines whether an attached Amazon EBS volume can be encrypted?
    a. The type of Amazon EC2 instance
    b. The size of the Amazon EBS volume
    c. The type of the Amazon EBS volume
    d. The IOPS assigned to the Amazon EBS volume

4. Where are data keys stored when they are delivered to an Amazon EC2 instance for safekeeping?
    a. The associated Amazon EBS volume
    b. Unsecured RAM
    c. Secured RAM
    d. AWS Key Management Service

5. What security policy allows multiple AWS accounts to access the same Amazon S3 bucket?
    a. Amazon IAM policy
    b. AWS IAM server control policy

c. Amazon S3 Bucket policy
d. Amazon IAM policy

6. What type of encryption can be carried out before uploading objects to Amazon S3 to ensure absolute encryption outside AWS control?
   a. RSA encryption
   b. AES 128-bit encryption
   c. Client-side encryption
   d. Server-side encryption

7. What is the advantage of importing your organization's symmetric keys into AWS KMS?
   a. High level of compliance
   b. Faster encryption and decryption
   c. Absolute control of encryption keys
   d. None

8. What additional AWS service can work with AWS KMS as a custom key store?
   a. Encrypted EBS volume
   b. Encrypted Amazon S3 bucket
   c. AWS CloudHSM
   d. Encrypted AWS SQS queue

9. How does AWS charge for provisioning SSL/TLS certificates for AWS services using AWS Certificate Manager?
   a. It charges per certificate per year.
   b. It charges for private TLS certificates only.
   c. It does not charge for AWS services.
   d. It charges per certificate check.

10. Where are the security certificates for the AWS Application Load Balancer stored?
    a. Amazon S3 bucket
    b. Amazon EBS volume
    c. AWS Certificate Manager
    d. AWS KMS service

Foundation Topics

Data Access and Governance

Many on-premises and AWS-hosted workloads store their associated data records in the AWS cloud. Personal data stored in the public cloud is sometimes defined as personally identifiable information (PII). Sensitive data types, such as PII, must be protected to comply with privacy regulations such as the General Data Protection Regulation (GDPR), laws such as the Health Insurance Portability and Accountability Act (HIPAA), and industry standards such as the Payment Card Industry Data Security Standard (PCI DSS). More than 13 billion data records have been stolen since 2013, according to the *2022 Thales Data Threat Report* (https://cpl.thalesgroup.com/data-threat-report). AWS Artifact, located in the AWS Management console, provides on-demand access to all current AWS compliance and security reports, including Service Organization Control (SOC) and Payment Card Industry (PCI) reports and certifications from accreditation bodies validating the implementation and operating effectiveness of AWS security controls (see Figure 5-2).

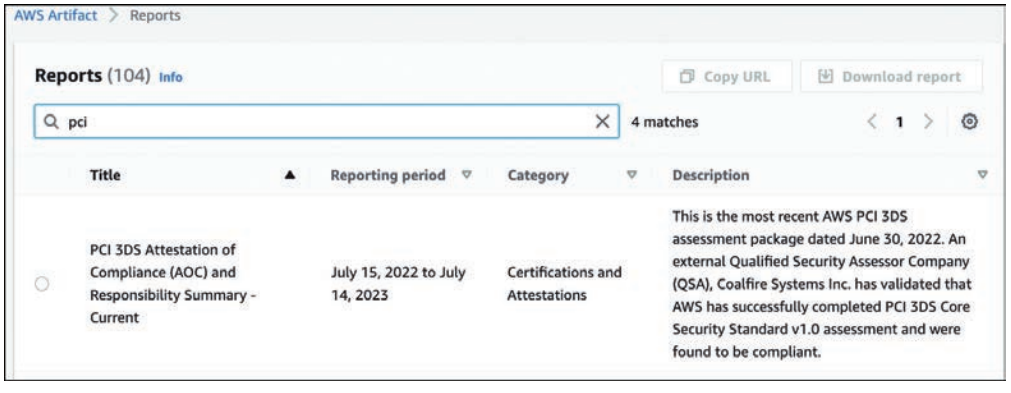

Figure 5-2 AWS Artifact PCI Report

Key Topic

Data Retention and Classification

When classifying data, it's important for each organization to implement data retention policies for each class of stored data. Organizations should design security policies using security zones for all data records, and data classification requirements based on how data is stored and who has access to it (see Figure 5-3). Defined security zones for data records range from highly protected to publicly accessible.

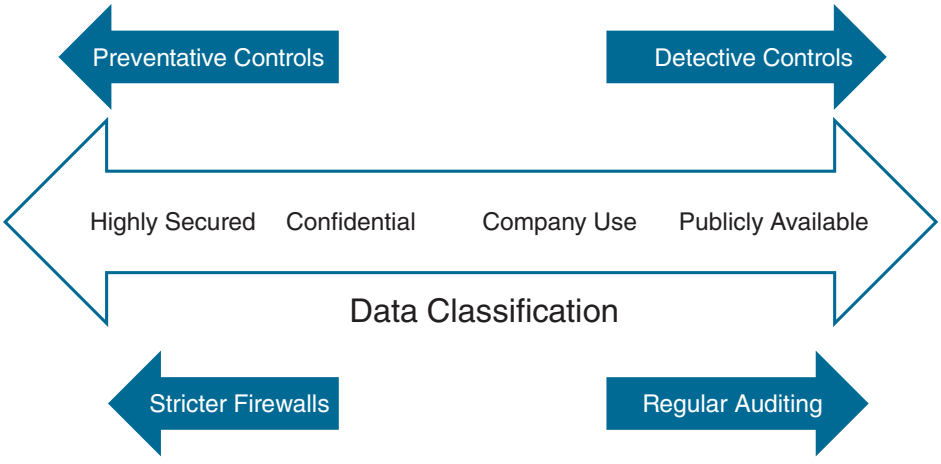

Figure 5-3 Classification of Data Records

Security zones are typically used to segregate different types of organizational data assets based on their sensitivity or importance, with the most sensitive or valuable data being placed in the highest security zone. This segregation enables organizations to implement different levels of security controls and access restrictions based on the sensitivity of the data, ensuring that only authorized users with the appropriate level of clearance can access and view sensitive data records.

Additionally, the creation of relevant security zones can help organizations prevent the spread of security breaches by limiting the potential impact to a specific area of the organization. Organizations also should create a network perimeter with defined network flow and access policies for data records defining where and how data can be accessed. Defense-in-depth security at AWS is applied using infrastructure security controls, AWS IAM security policies, and AWS detective controls (see Figure 5-4).

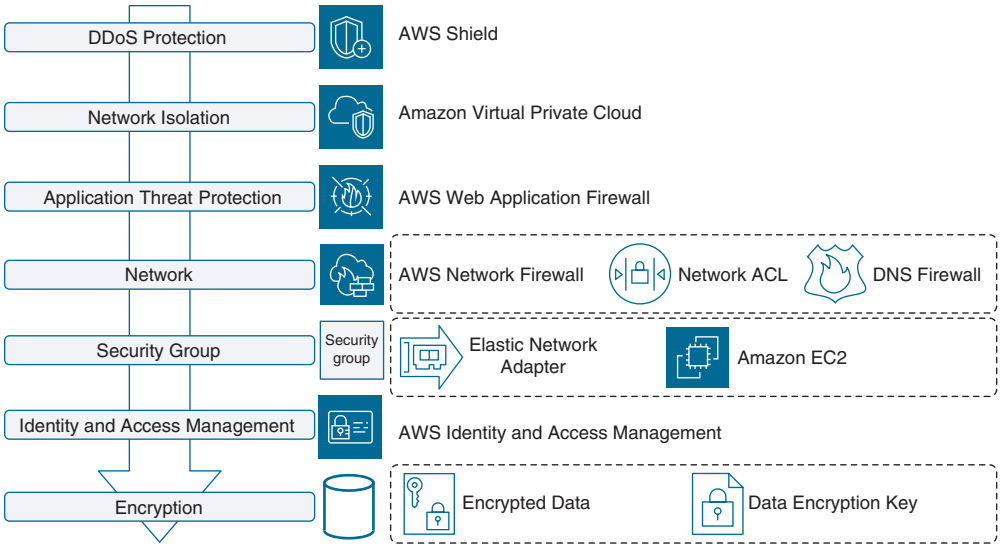

Figure 5-4 Preventative Controls

Key Topic

Infrastructure Security

Infrastructure security requires deploying the following protections:

- **DDoS Protection:** Amazon deploys AWS WAF and Shield to protect the AWS cloud from DDoS attacks.
- **Network isolation:** EC2 instances must be hosted in a virtual private cloud (VPC). Many AWS services can be accessed from a VPC with private VPC endpoints (Interface and Gateway endpoints), ensuring workload traffic remains on the private AWS network.
- **Application-layer threat protection:** The AWS Web Application Firewall (WAF) allows organizations to create rules and filters to accept or reject incoming requests to Amazon CloudFront distributions, Amazon API Gateway deployments, and Application Load Balancers, and HTTP/HTTPS traffic to web servers.
- **Security groups:** Security groups must be designed to allow ingress traffic from associated security groups.
- **Network ACL:** Design network ACLs to implement zone-based models for your workload (web/app servers/database), allowing only legitimate traffic to reach each subnet.

IAM Controls

AWS Identity and Access Management (IAM) policies are useful for controlling access to the data layer (database, queue, AWS EBS volumes, shared data [AWS EFS and AWS FSx for Windows File Server], and Amazon S3 storage) and managing IAM user and federated user activity and infrastructure security. Separate administrative tasks should be created for Amazon RDS with IAM policies (see Example 5-1) that control access to database data records. For authentication and authorization to any workload or organizational data records, enable multifactor authentication (MFA) for all administrators and end users.

Example 5-1 Administrative Access to Amazon RDS

```
"Version": "2012-10-17",
    "Statement": [
        {
            "Sid": " Controlled Admin Tasks",
            "Effect": "Allow",
            "Action": [
                "rds:CreateDBSnapshot",
                "rds:StopDBInstance",
                "rds:StartDBInstance"
            ],
            "Resource": [
                "arn:aws:rds:[AWS_region]:[_AWS_account_
id]:snapshot:*",
                "arn:aws:rds:[AWS_region]:[_AWS_account_
id]:db:demoDB"
            ]
        },
        {
            "Sid": "DescribeInstances",
            "Effect": "Allow",
            "Action": "rds:DescribeDBInstances",
            "Resource": "*"
        }
    ]
}
```

Detective Controls

Detective controls are a type of security control designed to detect and alert when potential security incidents or breaches occcur. Detective controls typically are used

with preventive and corrective controls forming a comprehensive security strategy. Examples of detective controls at AWS include intrusion detection systems, and auditing or logging systems that monitor user activity and alert on suspicious behavior. The goal of detective controls is to identify potential security threats or vulnerabilities before they can cause harm, allowing organizations to take appropriate action to prevent or mitigate the impact of a security incident.

Detective controls are an important part of a defense-in-depth security strategy as they provide an additional layer of protection by detecting and responding to potential security threats. Detective controls at AWS include the following security services:

- **VPC Flow Logs:** A feature of Amazon VPC that monitors network traffic at the elastic network interface, subnet, or entire VPC. Captured network traffic can be used for troubleshooting connectivity issues and to check current network access rules.
- **AWS CloudTrail:** Continuously monitor and record API usage and user activity across AWS infrastructure.
- **AWS CloudWatch:** Monitors AWS cloud services such as Amazon RDS databases, EC2 instances, and DynamoDB tables and hosted applications by collecting and tracking metric data, application and operating system log files, and using automated responses to defined alarms.
- **Amazon GuardDuty:** Provides continuous threat detection and analysis of VPC Flow Logs, Amazon Route 53 DNS query logs, and AWS CloudTrail S3 data event logs, and protecting AWS accounts and data stored in Amazon S3 from malicious activity. AWS GuardDuty malware protection can help detect malicious files stored on EBS volumes, protecting attached EC2 instances and Amazon Elastic Kubernetes Service (EKS) clusters.
- **AWS Config:** Detects configuration changes in RDS AWS infrastructure including Amazon RDS, EC2 instances, VPC and database architecture, including security groups, database instances, snapshots, and subnet groups.
- **Amazon Macie:** Uses machine learning and pattern matching to protect Amazon S3 objects and sensitive data types.
- **Access Analyzer for S3:** Monitors Amazon S3 buckets and details public or cross-account access.
- **Amazon Detective:** Graphically analyzes AWS CloudTrail management events, VPC Flow Logs, AWS GuardDuty findings, and Amazon EKS audit logs to help identify the cause of potential security issues.

Key Topic

Amazon EBS Encryption

Amazon Elastic Block Storage (EBS) volumes provide persistent block-level storage volumes for EC2 instances. They can be used to store a wide variety of data, including operating system files, application data, and database records. EBS volumes are automatically replicated within their availability zone to protect against data loss due to failure, and support a range of performance levels and storage options to meet the needs of different workloads.

Amazon Elastic Block Store (EBS) provides the option to encrypt EBS volumes to protect the data records. Encrypting EBS volumes ensures that the data cannot be read or accessed by unauthorized parties, even if the underlying storage volume is compromised. Encryption is performed using a customer master key and data key managed by the AWS Key Management Service (KMS), which provides a secure and auditable encryption service for managing data encryption at AWS using encryption keys. EBS volumes can be encrypted when first created, or volumes can be encrypted after they have been created. EBS also provides the option to encrypt snapshots of EBS volumes, enabling you to create encrypted backups of your EBS volumes.

Both EBS boot and data volumes can be encrypted. Most EC2 instances support EBS volumes' encryption, including the C4, I2, I3, M3, M4, R3, and R4 families. AWS has made the encryption process incredibly easy to deploy; when creating an EBS volume, merely checking off the option to enable encryption starts the encryption process (see Figure 5-5), which is managed by AWS Key Management Service (KMS). More details on AWS KMS are provided throughout this chapter.

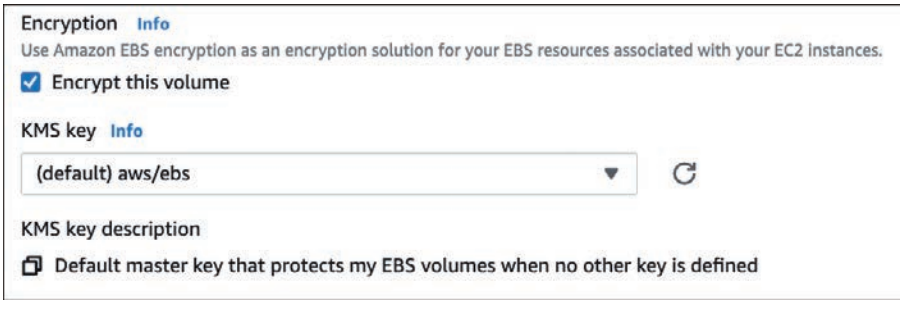

Figure 5-5 Enabling EBS Encryption

NOTE Data encrypted using the EBS encryption process is encrypted before it crosses the AWS private network. Data also remains encrypted in-flight and at rest and remains encrypted when a snapshot is created of an encrypted volume.

The CMK protects all the other keys issued for data encryption and decryption of your EBS volumes within your AWS account. All AWS KMS-issued CMKs are protected using envelope encryption, which means AWS is responsible for creating and wrapping the "envelope" that contains the CMKs of the respective AWS account. Envelope encryption encrypts the plaintext data with a data key, and then encrypts the data key using a key that is managed by the AWS Key Management Service (KMS). KMS keys are created inside AWS KMS and never leave AWS KMS unencrypted. AWS cryptographic tools and services support the Advanced Encryption Standard (AES) with 128-, 192-, or 256-bit keys. AES is combined with Galois/Counter Mode (GCM), which provides high-performance ***symmetric key*** operation using a block size of 128 bits and is used by AWS KMS. AES and GCM are documented as AES-GCM.

After enabling your customer key using KMS for your AWS account, for additional security, it's a good idea to add another key administrator and to allow key rotation of your Customer Master Keys. Administrators can use the KMS master key provided to create additional AWS KMS administrators, and to optionally enable key rotation of the CMK (see Figure 5-6).

Key Topic

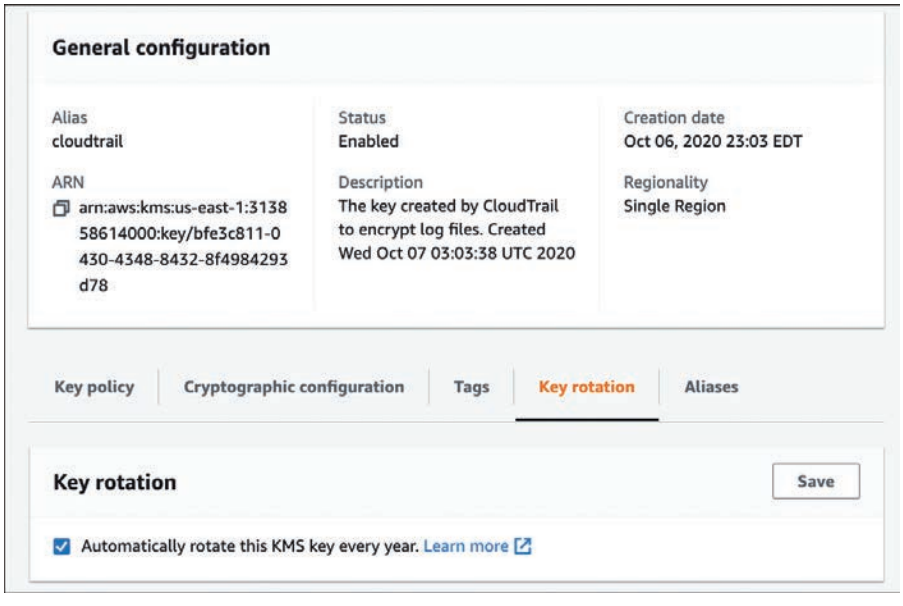

Figure 5-6 Enabling Key Rotation

To encrypt an EBS volume using the AWS Key Management Service, a CMK can be created by AWS and stored in AWS KMS. Optionally, organizations can choose to specify the key material for the CMK, which can be generated by KMS or imported from your own key management infrastructure. After a CMK has been created, you

can create an encrypted EBS volume using the EC2 dashboard and specifying the ID of the CMK when creating the volume (see Figure 5-7). The EBS volume will be encrypted using the specified CMK, and the data on the EBS volume will be encrypted at rest on the underlying storage.

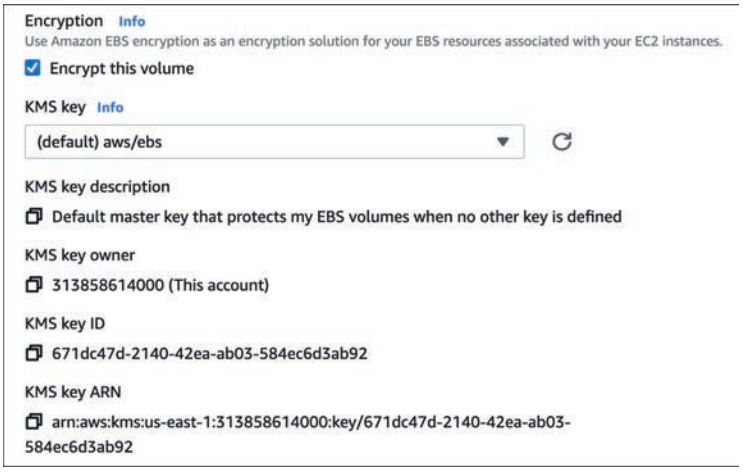

Figure 5-7 Select KMS Key

When you attach the encrypted EBS volume to an EC2 instance, the instance will automatically download and install the necessary encryption and decryption components, including the appropriate version of the AWS Encryption SDK and the public key portion of the CMK. The instance will then use the CMK to encrypt and decrypt data as it is written to and read from the EBS volume. The private key portion of the CMK remains securely stored in AWS KMS, and is never made available to the EC2 instance.

When an EBS volume has been encrypted and attached to an EC2 instance, the following data types are encrypted:

- Data at rest inside the EBS volume
- All data that moves between the attached EBS volume and the EC2 instance
- All snapshots created from the EBS volume
- All volumes created from the encrypted snapshots

AWS KMS performs the following steps, as illustrated in Figure 5-8, to encrypt and decrypt the EBS volume:

Step 1. AWS EBS sends a request to KMS, specifying the CMK to use for the AWS EBS volume encryption.

Step 2. AWS KMS generates a new data key, encrypts it using the specified CMK, and sends the encrypted key to AWS EBS to be stored with the volume metadata.

Step 3. The Amazon EC2 service sends a decrypt request to KMS.

Step 4. EBS sends a request to KMS to decrypt the data key.

Step 5. KMS uses the CMK to decrypt the encrypted data key and sends the decrypted key to the EC2 service.

Step 6. EC2 stores the plaintext decrypted key in protected hypervisor memory on the bare-metal server where the EC2 instance is hosted and uses the key when required to perform decryption for the EBS volume.

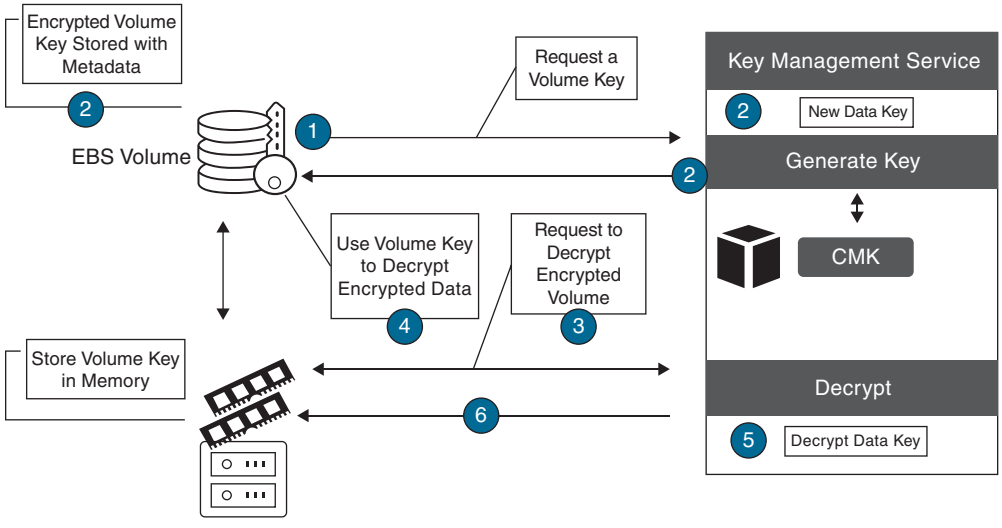

Figure 5-8 EBS Encryption Steps

NOTE The default setting for each AWS region is that EBS encryption is not enabled. To enable EBS encryption in the AWS region, open the EC2 dashboard, and in the upper-right corner under Account Attributes click EBS Encryption. Click Manage and choose the desired AWS-managed CMK or another CMK. Next, click Enable and then click Update EBS encryption. Once encryption is enabled for the AWS region, all new EBS volumes and snapshots will be encrypted at creation.

Amazon S3 Bucket Security

By default, only the owner who created an S3 bucket has access to the objects stored in the bucket. There are several methods for controlling security for an S3 bucket (see Figure 5-9):

- **ACLs:** You can use ***access control lists (ACLs)*** to control primary access from other AWS accounts for list and write objects and read and write bucket permissions, public access, and access to S3 logging information. ACLs are available for purposes of backward compatibility and are the weakest type of S3 security (and therefore not recommended).

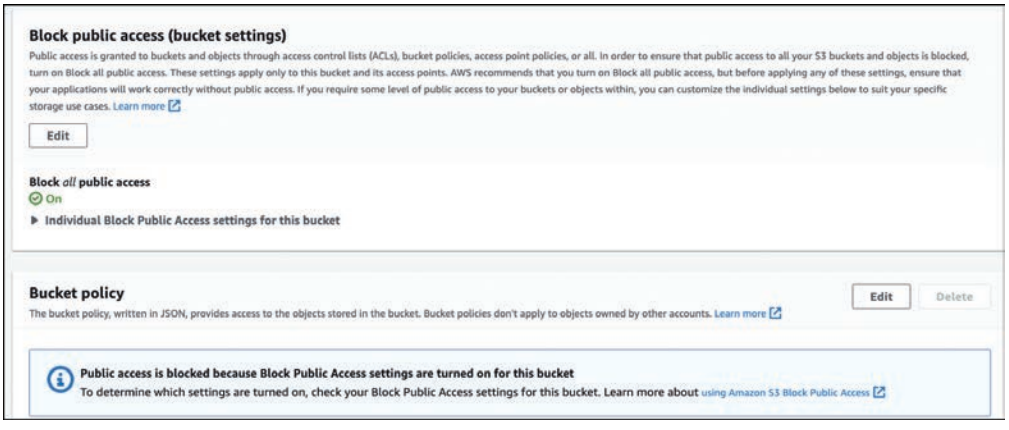

Figure 5-9 S3 Permission Settings

- **IAM policy:** You can grant access to other AWS users and groups of IAM users by using IAM permission policies in partnership with resource policies.
- **S3 Bucket policy:** You can control direct access to an S3 bucket, as shown in Example 5-2, by creating a ***bucket policy*** assigned directly to the S3 bucket. An S3 bucket policy is a JSON-formatted document that defines which actions are allowed or denied on an S3 bucket and its contents. A bucket policy is attached directly to the bucket it is protecting, and the policy settings list who has access to the bucket and what they can do with the objects in the bucket. An S3 bucket policy might allow a specific IAM user to read and write objects in the bucket, while denying access to all other users. Or, the policy might allow any user to read objects in the bucket but allow only authenticated users to write objects.

S3 bucket policies are defined using the AWS Policy Language, which provides a set of keywords and operations that you can use to specify the conditions under which a policy takes effect. A bucket policy can also allow access from multiple AWS accounts to a single S3 bucket.

Example 5-2 S3 Bucket Policy

```
{
  "Version": "2012-10-17",
  "Id": "S3PolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": [
                    "arn:aws:s3:::2021232reports",
         "arn:aws:s3:::2021232reports/*"
      ],
      "Condition": {
          "NotIpAddress": {"aws:SourceIp": "54.242.144.0/24"}
      }
    }
  ]
}
```

- **Query string authentication:** Query string authentication is a method to authenticate requests to an Amazon S3 bucket allowing organizations to generate a URL (see Figure 5-10) that can be shared with end users. When an end user clicks the URL, they are granted access to the specified S3 bucket and its contents.

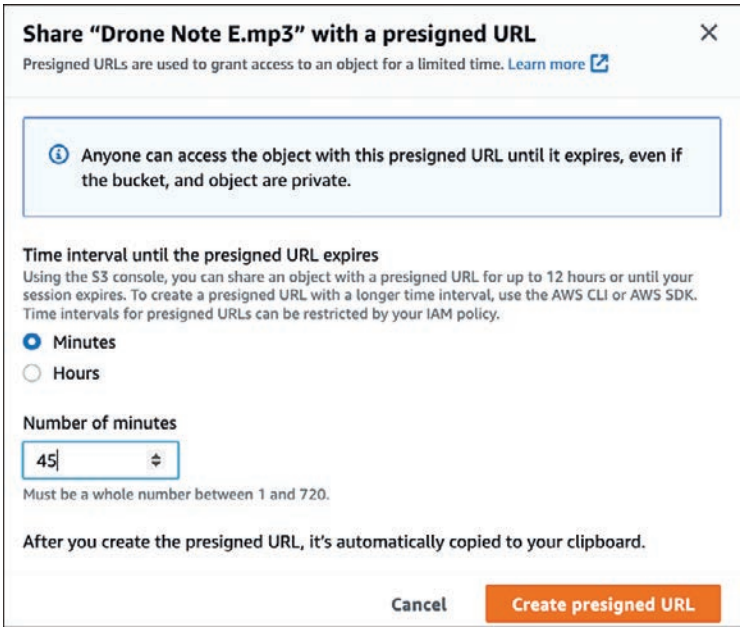

Figure 5-10 Presigned URL for S3 Object Access

The URL includes a set of parameters that specify the credentials that grant access to the bucket. These parameters include the access key ID, an expiration time for the URL, and a signature that is calculated using the access key secret.

When someone attempts to access the URL, the Amazon S3 service checks the signature to verify that it matches the expected value. If the signature is valid, the user is granted access to the bucket; otherwise, the request is denied.

The use case for using query string authentication is useful for granting temporary access to an S3 bucket without having to create an IAM user or provide AWS access keys. However, query string authentication is not as secure as IAM policies or bucket policies because the URL and its parameters are included in each request; therefore, anyone who has access to the URL can potentially gain access to the bucket.

NOTE If you require public access to objects in an S3 bucket, it's recommended that you create a separate AWS account specifically for hosting the S3 buckets that will have public S3 object access.

- **Blocking S3 public access:** S3 Buckets always start as private, with no default public access (see Figure 5-11). When the Block Public Access (Bucket Settings) setting is enabled, attempts at changing security settings to allow public access to objects in the S3 bucket are denied. You can block public access on an individual S3 bucket or on all S3 buckets in your AWS account by editing the public access settings for your account using the S3 console. Choices for blocking S3 public access include the following:
  - **Public:** Everyone has access to list objects, write objects, and read and write permissions.
  - **Objects Can Be Public:** The bucket is not public; however, public access can be granted to individual objects by users with permissions.
  - **Buckets and Objects Not Public:** No public access is allowed to the bucket or the objects within the bucket.

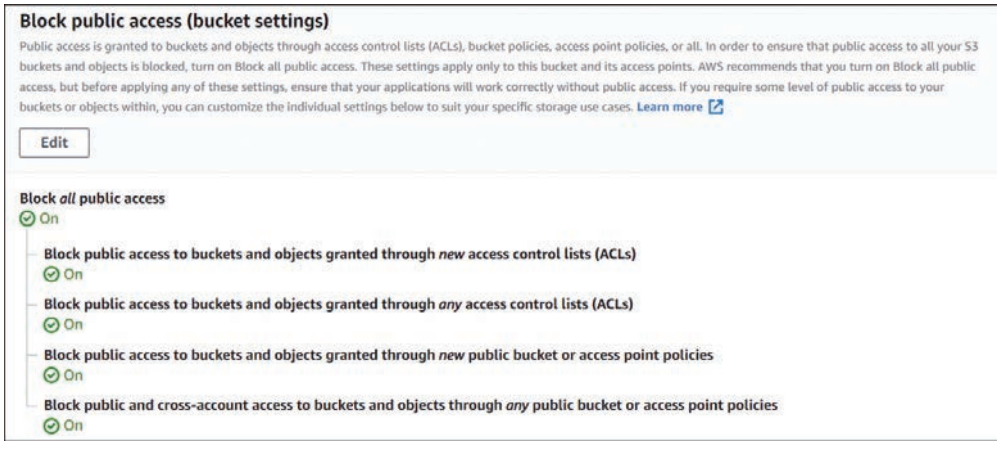

Figure 5-11 Blocking Public Access on an S3 Bucket by Default

NOTE Amazon Macie is a powerful AWS security service that uses artificial intelligence (AI) and machine learning (ML) technology to analyze your S3 objects and access patterns. Amazon S3 data can be classified based on many file formats, such as Personally Identifiable Information (PII) and other file types. AWS SNS notifications can be generated by Amazon Macie when Amazon S3 objects are discovered to be compromised.

Key Topic

S3 Storage at Rest

For the AWS Certified Solutions Architect – Associate (SAA-C03) exam, the key topics to know about S3 storage at rest are as follows:

- **SSE-S3:** With SSE-S3, Amazon S3 manages the encryption and decryption of the data in the bucket. Organizations that select this option don't manage the encryption keys but can access the data in the bucket without having to manage the keys. SSE-S3 uses the Advanced Encryption Standard (AES) algorithm with a 256-bit key to encrypt the data in the bucket. The key is automatically generated by Amazon S3 and is regularly rotated to ensure the security of the encrypted data (see Figure 5-12). Note that SSE encrypts the object data but the optional tag object metadata remains unencrypted.

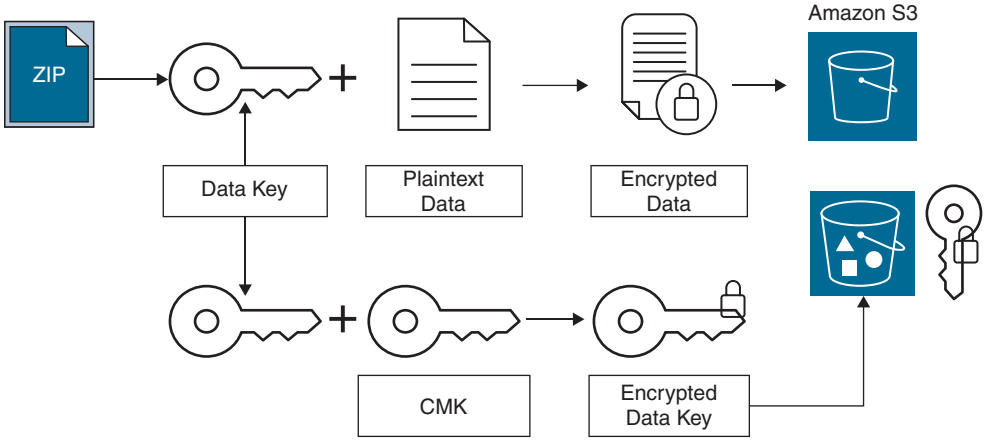

Figure 5-12 SSE-S3 Encryption Process

- **SSE-KMS:** Organizations can select AWS KMS to manage their encryption keys. Select the default CMK or choose a CMK that was already created in AWS KMS before starting an S3 encryption process. Accessing encrypted objects managed by KMS can be expensive: If you have an exceptionally large number of encrypted objects, a large volume of decryption requests will be made to KMS. You can configure SSE-KMS to significantly reduce the cost of the encryption and decryption process. When an S3 Bucket Key is configured for SSE-KMS server-side encryption, a short-lived encryption key is created and stored and used to encrypt objects internally inside AWS S3 rather than utilize AWS KMS encryption processes. The S3 Bucket Key creates unique data keys for encrypting objects in the specific S3 bucket that has enabled the S3 Bucket Key option. The encryption process reduces AWS KMS requests

for external encryption keys and can reduce encryption costs by 99%. The S3 Bucket Key is a worker process within the S3 bucket that enables you to perform encryption services without constant communication with KMS.

- **SSE-C:** You can use SSE with a customer-provided encryption key. With each request, the encryption key is provided to AWS, and Amazon S3 manages the encryption and decryption of S3 objects by using the supplied key. The same encryption key that was used to encrypt the object must be provided before the object can be decrypted (see Figure 5-13). After the encryption process is complete, the supplied encryption key is deleted from memory. To upload an object with an organization-provided encryption key (SSE-C), the AWS CLI, AWS SDK, or Amazon S3 REST API must be used.

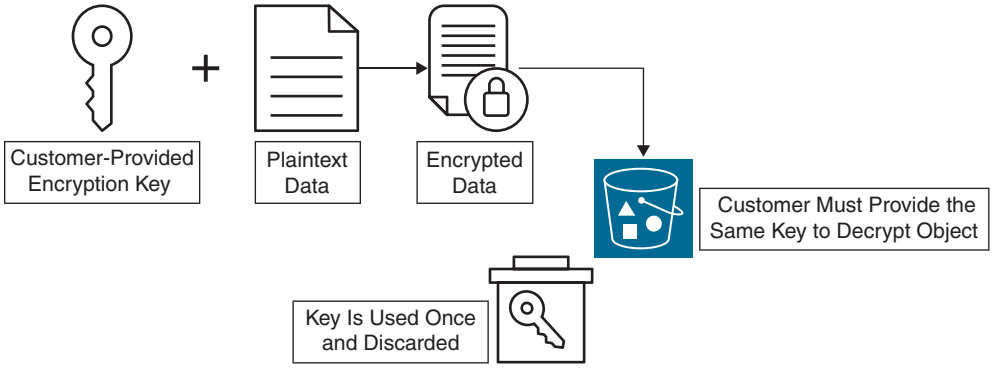

Figure 5-13 SSE-C Encryption Process

Key Topic

Amazon S3 Object Lock Policies

Amazon S3 buckets and Amazon S3 Glacier have data policies that can lock objects so they cannot be deleted or changed. Amazon S3 objects can be locked using a ***write-once/read-many (WORM)*** policy. Object lock policies enable you to set rules that restrict certain actions on objects, such as deleting or overwriting them, in order to protect objects and ensure they remain available and unaltered. Object lock policies are set at the S3 bucket level and apply to all objects in the bucket, or set on individual objects. This can be useful for complying with legal or regulatory requirements or protecting important or sensitive data. Apply a WORM policy, as shown in Figure 5-14, to stop an Amazon S3 object from being overwritten, or deleted for a fixed time period, or indefinitely. There are several options to WORM policies to understand. First is the *retention period*, which refers to a set number of days or years during which an object will remain

locked, protected, and unable to be overwritten or deleted. There are two retention modes:

- **Governance mode:** An S3 object cannot have its lock settings overwritten and cannot itself be overwritten or deleted unless the user has unique permissions. To override governance mode retention settings, an IAM user must have the **s3: BypassGovernanceRetention** permission and **x-amz-bypass-governance-retention: true** applied.
- **Compliance mode:** A protected object in your AWS account cannot be overwritten or deleted by anyone, including the root user, for the entire retention period.

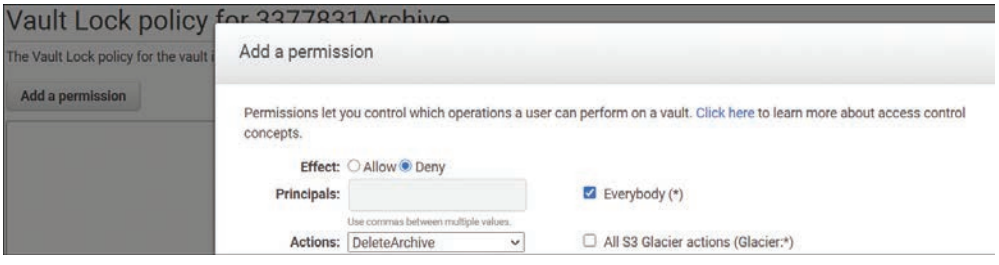

Figure 5-14 WORM Policy Settings

Legal Hold

An object lock allows you to place a legal hold on an S3 object. Legal hold provides the same protection as a previously discussed retention period but does not have an expiration date. expiration date. Once in force, a legal hold remains in place until it is removed. An object lock works on S3 buckets that have versioning already enabled. Legal hold can be applied to a single S3 object. A legal hold can be placed and removed by any user with the **s3:PutObjectLegalHold** permission applied to their IAM user or group account they are a member of.

NOTE Object lock can only be enabled for new buckets when they are being created.

Key Topic

Amazon S3 Glacier Storage at Rest

Objects stored in Amazon S3 Glacier are automatically encrypted using SSE and AES-256 encryption. Amazon S3 Glacier Vault Lock enables you to deploy and

enforce regulatory and required compliance controls by applying a Vault Lock policy on an Amazon S3 Glacier vault. Once a WORM policy has been applied to an S3 Glacier vault, the policy cannot be changed.

NOTE Both EFS and FSx use AES-256 encryption to encrypt EFS data and metadata at rest. When your file system is mounted, you can also encrypt your EFS data in transit with TLS. FSx also supports the encryption of data in transit on file shares mapped on a computer instance that supports SMB Version 3.0 or newer. Encryption of data records at rest is automatically enabled when an FSx file system is created.

Data Backup and Replication

Amazon S3 object backups can be carried out with the services and utilities listed in Table 5-2. AWS Backup and AWS DataSync can back up additional AWS storage service data records.

Table 5-2 Data Backup and Replication Options

AWS Service	Use	Data Types
AWS Backup	Back up all AWS storage services	EBS volumes and snapshots, S3 buckets, EFS, FSx for Windows File Server, RDS, DynamoDB
Amazon S3 Same-Region Replication (SRR)	Replicate objects to an S3 bucket in the same AWS region	Objects and versioned objects
Amazon S3 Cross-Region Replication (CRR)	Replicate objects to an S3 bucket in a different AWS region	Objects and versioned objects
Amazon S3 Multi-Region Access Points	Replicate data sets across multiple AWS regions	Objects and versioned objects
AWS DataSync	Copy data to and from AWS storage services	Network File System (NFS) or Server Message Block (SMB) shares, Hadoop Distributed File Systems (HDFS), AWS Snowcone, S3 buckets, EFS, FSx for Windows File Server

AWS Key Management Service

Key Topic

AWS Key Management Service (KMS) lets organizations create, manage, and control cryptographic keys used to protect data records. AWS KMS integrates with AWS services that can encrypt data records (see Figure 5-15).

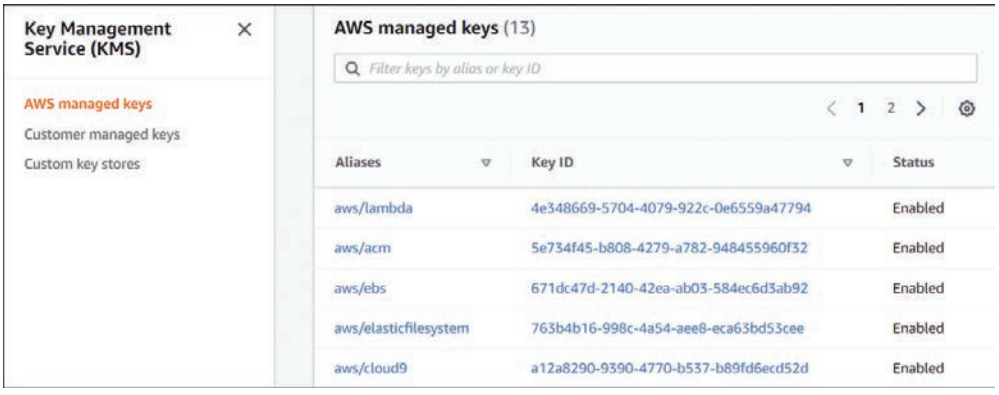

Figure 5-15 KMS Console

Organizations do not have to directly interface with AWS KMS to enable data encryption; instead, they can use AWS KMS services through more than 100 integrated AWS services, such as Amazon EBS storage, Amazon RDS, Amazon S3, Amazon EFS, Amazon FSx for Windows File Server, Amazon Aurora, and Amazon DynamoDB. When you enable encryption services using AWS KMS, a CMK is automatically generated in your AWS account for data encryption and decryption services. Organizations can choose to create one or more CMKs and use them to match their security requirements. A custom CMK allows you to control each key's access control and usage policy; you can also grant permissions to other AWS accounts and services to use a specific custom CMK.

You can also choose to create symmetric CMKs, which use the same key to encrypt and decrypt data, or asymmetric CMKs, which use a public/private key pair (one for encrypting and one for decrypting).

The most common way to use KMS is to choose which AWS service will encrypt your data and select the CMK from within the AWS service itself; for example, you can encrypt an RDS database volume, as shown in Figure 5-16.

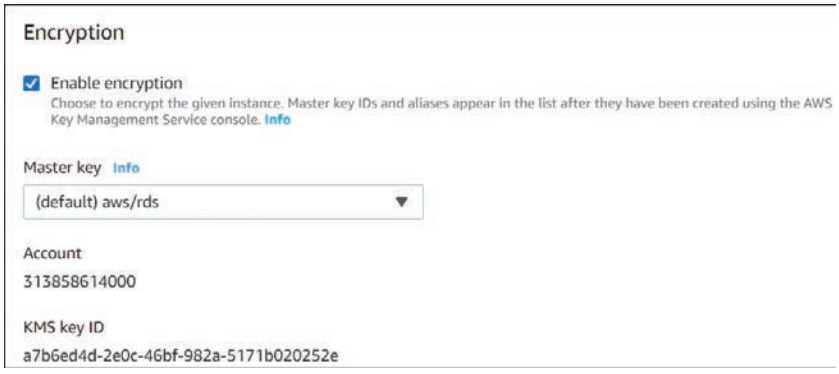

Figure 5-16 Generating CMKs with KMS for an RDS Instance

Envelope Encryption

KMS uses a process called *envelope encryption* to encrypt data at rest. It involves two layers of encryption: the first layer encrypts the data using a key generated by the organization, and the second layer encrypts the customer-generated key using a key that is managed by the AWS Key Management Service (KMS). This process enables each organization to retain control over their encryption keys and also enables them to rotate and manage the keys as needed, while still benefitting from the security and reliability of using the KMS for encryption key management. When you need to encrypt data, KMS generates a data key that is used to encrypt the data locally within the AWS service or application. The data keys are also encrypted under the organization's CMK. When it's time to decrypt your data, a request is sent to KMS to decrypt the data key (that is, the data key copy that was stored with the encrypted data) using your CMK. The entire encryption or decryption process is logged in AWS CloudTrail for auditing purposes.

NOTE You can create up to 10,000 CMKs per AWS account per AWS region. Keys generated by AWS KMS can be enabled to be automatically rotated on an annual basis. However, automatic key rotation is not supported for external cryptographic keys imported into AWS KMS.

Organizations that choose to import 256-bit symmetric keys into AWS KMS for compliance requirements are responsible for managing the imported keys' expiration dates.

In addition to encrypting your data, AWS KMS provides other security features to help protect your encryption keys:

- **Key management:** As an administrator, you can create, rotate, disable, and delete the CMKs that are used to encrypt your data. You can also view the key policy for a CMK, which specifies who has access to the CMK and what actions they can perform with it.
- **Access control:** Organizations can use AWS IAM policies to control who has access to their CMKs and what actions can be performed with them. For example, users can be granted the ability to encrypt data using a specific CMK, but not to decrypt it or change the key policy.
- **Auditing:** AWS KMS logs all API calls to AWS CloudTrail so organizations can track who is using each CMK and for what purpose. Auditing can help ensure that encryption keys are being used securely and in accordance with an organization's security policies.
- **Key material:** KMS stores the key material for your CMKs in secure hardware devices called hardware security modules (HSMs). This helps protect the security of each organization's keys and ensures that they are only accessible to authorized users.
- **Key rotation:** CMKS can be configured to automatically be rotated on an annual basis, to help prevent security breaches.

AWS KMS Cheat Sheet

For the AWS Certified Solutions Architect – Associate (SAA-C03) exam, you need to understand the following critical aspects of AWS KMS:

- AWS KMS can be used to create symmetric keys within a custom key store such as AWS CloudHSM.
- An organization's symmetric keys can be imported for use with AWS KMS.
- AWS KMS can create symmetric and asymmetric data key pairs for application use.
- CMKs can be automatically rotated annually.
- CMKs can be disabled and re-enabled.
- AWS KMS keys can be audited with AWS CloudTrail.

Key Topic

AWS CloudHSM

Instead of using the default AWS KMS store, you can create a custom key store using a VPC-hosted AWS CloudHSM cluster and authorize KMS to use it as its dedicated key store. AWS CloudHSM clusters are created using multiple single-tenant hardware devices (see Figure 5-17). Amazon maintains the AWS CloudHSM hardware and backs up its contents but never enters an AWS CloudHSM device. Organizations might use an AWS CloudHSM deployment if compliance rules explicitly require that encryption keys are protected in a single-tenant hardware device. AWS CloudHSM can operate as a complete stand-alone hardware device for your synchronous and asynchronous keys and provide you with Federal Information Processing Standard (FIPS) 140-2 Level 3 compliance.

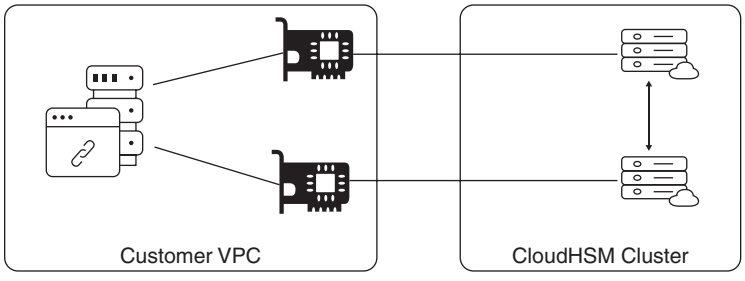

Figure 5-17 CloudHSM Design

AWS Certificate Manager

AWS Certificate Manager (ACM) is a managed service that allows you to provision, manage, and deploy public and private SSL/TLS certificates that can be used with your AWS services and AWS-hosted websites and applications. Certificates can also be deployed on ELB load balancers, CloudFront distributions, Elastic Beanstalk, and APIs hosted on Amazon API Gateway. There is no additional charge for provisioning public or private SSL/TLS certificates for use with AWS services. However, organizations will pay a fee for creating and operating a private ***certificate authority (CA)*** and for the private certificates that are issued by the private CA that is used by your internally hosted resources, such as application servers or appliances.

ACM can generate the following certificate types (see Figure 5-18):

Key Topic

- **Public certificates:** ELB port 443 traffic, CloudFront distributions, and public-facing APIs hosted by Amazon API Gateway all use public certificates. Use AWS Certificate Manager to request a public certificate for a domain name for your site. AWS Certificate Manager validates that you own or control the domain name in your certificate request. Validation options include DNS validation and email validation.

- **Private certificates:** Delegated private certificates are managed by an AWS Certificate Manager–hosted private CA, which can automatically renew and deploy certificates for private-facing Amazon ELB and Amazon API Gateway deployments. Private certificates can also secure Amazon EC2 instances, Amazon ECS containers, and IoT devices.
- **Imported certificates:** Third-party certificates can be imported into AWS Certificate Manager.
- **CA certificates:** Certificates can be issued for creating a private CA up to five levels deep, including a root CA, three levels of subordinate CAs, and a single issuing CA.

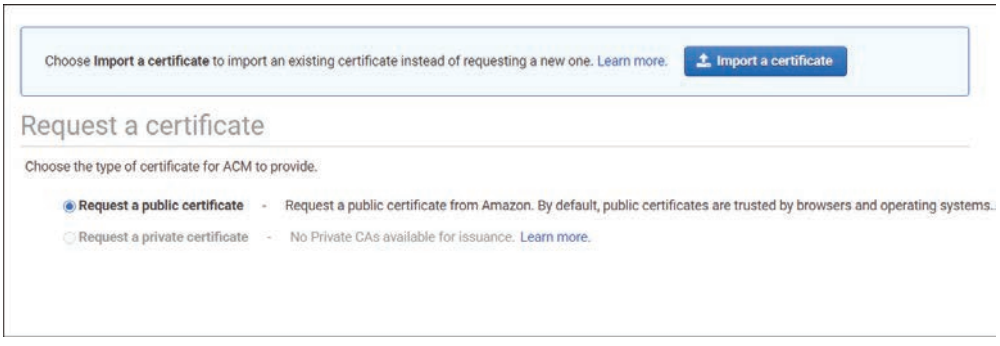

Figure 5-18 Certificate Choices in AWS Certificate Manager

Encryption in Transit

AWS uses HTTPS endpoints communication, providing encryption in transit for communicating with AWS APIs. AWS service endpoints can also be accessed using TLS version 1.2. Some AWS services offer endpoints that support the Federal Processing Standard (FIPS) 140-2 in some regions. Each endpoint is the URL of the entry point for each AWS service. AWS SDKs and the AWS Command Line Interface (AWS CLI) automatically use the default endpoint for each service per AWS Region, but an alternative endpoint can be specified for API requests. Most AWS services have regional endpoints that can be used to make requests. The format for a regional endpoint is *protocol://service-code.region-code*.amazonaws.com. AWS endpoints can be referenced here: https://docs.aws.amazon.com/general/latest/gr/aws-service-information.html.

Global endpoints are used for global services and services located in edge locations. The global AWS services are

- Amazon CloudFront
- AWS Global Accelerator

- AWS Identity and Access Management (IAM)
- AWS Organizations
- Amazon Route 53
- AWS Shield Advanced
- AWS WAF Classic

HTTP endpoints for domains and hosted workloads hosted at AWS can be be blocked with Security Groups and Network ACLs and can automatically be redirected to HTTPS endpoints when using Amazon CloudFront or an Amazon ELB.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of 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 the chapter, noted with the Key Topic icon in the margin of the page. Table 5-3 lists these key topics and the page number on which each is found.

Key Topic

Table 5-3 Chapter 5 Key Topics

Key Topic Element	Description	Page Number
Figure 5-1	Encryption Choices at AWS	204
Section	Data Retention and Classification	207
Section	Infrastructure Security	209
Section	Detective Controls	210
Section	Amazon EBS Encryption	212
Figure 5-6	Enabling Key Rotation	213
Section	S3 Storage at Rest	220
Section	Amazon S3 Object Lock Policies	221
Section	Amazon S3 Glacier Storage at Rest	222

Key Topic Element	Description	Page Number
Section	AWS Key Management Service	224
Section	AWS KMS Cheat Sheet	226
Section	AWS CloudHSM	227
List	AWS Certificate Manager certificate types	227

Define Key Terms

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

Amazon Elastic Block Storage (EBS), symmetric key, access control list (ACL), bucket policy, write-once/read-many (WORM), AWS Key Management Service (KMS), certificate authority (CA)

Q&A

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

1. Which AWS storage service is available with AWS as a single-tenant storage design?
2. What is the default state of an S3 bucket regarding public access when the bucket is first created?
3. What is the security advantage of using SSE-C encryption with Amazon S3 buckets?
4. Describe the concept of envelope encryption that KMS uses.
5. What type of data stored at AWS is always automatically encrypted by default?
6. Why is AWS CloudHSM chosen by companies that must adhere to a high compliance standard?
7. How does AWS KMS carry out automatic key rotation for imported keys?
8. Where can private CAs created by AWS Certificate Manager be deployed?

This page intentionally left blank

Index

A

B

C

D

E

F

G

H

I

J-K

L

M

N

O

P

Q

R

S

T

U

V

W

X-Y-Z