AWS Certified Security Specialty SCS-C02 Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Table of Contents

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- **Practice answering questions under realistic conditions,**
- **Improve accuracy and speed,**
- **Review explanations to strengthen weak areas, and**
- **Approach the exam with greater confidence.**

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here’s how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don’t just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There’s no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

Questions

1. What AWS service helps detect abnormal or sudden spending increases in your account?

A. AWS Budgets

B. AWS Cost Explorer

C. AWS Cost Anomaly Detection

D. AWS Trusted Advisor

2. What is the purpose of AWS Secrets Manager?

A. To manage AWS billing and account costs

B. To securely store and manage sensitive information like passwords and API keys

C. To provide real-time data analysis for applications

D. To optimize cloud resource usage and performance

3. At which layer of the OSI model does the Network Load Balancer function?

A. Layer 3

B. Layer 4

C. Layer 5

D. Layer 7

4. What feature allows management of public access settings for S3?

A. S3 Block Public Access feature

B. Access Management feature

C. Public Access Control

D. S3 Permissions Manager

5. What are security headers in HTTP responses used for?

A. To encrypt the data transferred

B. To tell a browser how to handle site content

C. To authenticate users

D. To optimize performance

6. Which protocol does AWS IoT Core support for device connectivity?

A. HTTP/2

B. MQTT

C. WebSocket

D. FTP

7. Which of the following is a risk associated with not applying security patches promptly?

A. Increased operational costs

B. Higher chances of system outages

C. Exposure to vulnerabilities and exploits

D. Loss of hardware efficiency

8. Amazon Cognito serves as what type of service within AWS?

A. Data processing service

B. User directory and authentication server

C. Cloud storage solution

D. Serverless compute service

9. Which AWS service can be used to monitor API calls?

A. AWS CloudTrail

B. AWS Config

C. AWS Shield

D. AWS Inspector

10. Which service extracts, transforms, and delivers streaming data to various data stores and analytics services?

A. Amazon S3 Transfer Acceleration

B. Amazon Kinesis Data Firehose

C. AWS Direct Connect

D. AWS Data Pipeline

Answers

1. C
2. B
3. B
4. A
5. B
6. B
7. C
8. B
9. A
10. B

Explanations

1. What AWS service helps detect abnormal or sudden spending increases in your account?

A. AWS Budgets

B. AWS Cost Explorer

C. AWS Cost Anomaly Detection

D. AWS Trusted Advisor

The AWS service that specifically helps detect abnormal or sudden spending increases in your account is AWS Cost Anomaly Detection. This service utilizes machine learning models to monitor your spending patterns and identify any unusual charges that deviate from your typical expenditure trends. By setting up alerts, it notifies you when it senses a significant increase in costs, allowing you to take prompt action to mitigate unexpected expenses. While AWS Budgets allows you to set monetary and usage budgets and track your performance against these budgets, it does not specifically focus on detecting anomalies in spending. AWS Cost Explorer provides visualizations of your spending trends over time but lacks the automated anomaly detection feature. Likewise, AWS Trusted Advisor offers best practice recommendations for optimizing your AWS accounts, such as cost optimization, but it does not monitor spending patterns or detect anomalies directly. Hence, for the precise function of identifying unusual spending patterns, AWS Cost Anomaly Detection is the most appropriate choice.

2. What is the purpose of AWS Secrets Manager?

A. To manage AWS billing and account costs

B. To securely store and manage sensitive information like passwords and API keys

C. To provide real-time data analysis for applications

D. To optimize cloud resource usage and performance

AWS Secrets Manager is designed specifically to securely store and manage sensitive information such as passwords, API keys, and database credentials. It helps organizations safeguard their access information by enabling secure management and retrieval of secrets without embedding them in application code, which can lead to security vulnerabilities. Secrets Manager provides features like automatic rotation of secrets, fine-grained access control using AWS Identity and Access Management (IAM), and secure access within AWS services, which further enhances the security posture of applications using sensitive data. By centralizing the management of secrets, it reduces the risk of accidental exposure or misuse, thereby streamlining the overall handling of confidential information within the AWS cloud environment. The other options pertain to different functionalities not related to the core purpose of Secrets Manager, emphasizing that its primary role focuses on the protection and management of sensitive information.

3. At which layer of the OSI model does the Network Load Balancer function?

A. Layer 3

B. Layer 4

C. Layer 5

D. Layer 7

The Network Load Balancer (NLB) operates at Layer 4 of the OSI model, which is the Transport Layer. This layer is responsible for the transmission of data segments between systems. The NLB can handle millions of requests per second while maintaining ultra-low latencies, making it highly efficient for routing TCP and UDP traffic. By functioning at Layer 4, the NLB makes routing decisions based on IP address and TCP/UDP port numbers. This means it does not inspect the contents of the messages but instead focuses on the information that can be gleaned from the packet headers. This is crucial for its ability to rapidly distribute incoming traffic across multiple targets, increasing the availability and reliability of applications. In contrast, options associated with higher layers like Layer 7 deal with application-level data and include more complex processing, such as content-based routing and SSL termination. Layer 3, which focuses on network layer functionalities such as IP addressing, is also a lower level than where the NLB operates. Therefore, the choice of Layer 4 is justified for the functionalities offered by the Network Load Balancer.

4. What feature allows management of public access settings for S3?

A. S3 Block Public Access feature

B. Access Management feature

C. Public Access Control

D. S3 Permissions Manager

The S3 Block Public Access feature is specifically designed to manage the public access settings for Amazon S3 buckets and objects. This feature allows administrators to enforce account-wide or bucket-specific settings that prevent public access, which is crucial for ensuring that sensitive or private data stored in S3 is not unintentionally exposed to the internet. The S3 Block Public Access feature provides granular controls that allow you to block all public access to buckets and objects or only allow certain exceptions based on your security needs. This is essential for compliance and security best practices, as it helps prevent data leaks by ensuring that only authorized users can access the resources. In contrast, other options mentioned do not specifically address managing public access in the same comprehensive way. Access Management focuses on broader permissions and role-based access, while Public Access Control and S3 Permissions Manager are not formal terms used by AWS to describe specific capabilities relevant to managing public access. Thus, the S3 Block Public Access feature is the most accurate and effective tool for this purpose.

5. What are security headers in HTTP responses used for?

A. To encrypt the data transferred

B. To tell a browser how to handle site content

C. To authenticate users

D. To optimize performance

Security headers in HTTP responses play a crucial role in guiding web browsers on how to handle content securely, making option B the correct choice. These headers are primarily designed to enhance the security of web applications by specifying policies related to various security aspects. For example, headers such as Content Security Policy (CSP) instruct the browser on which resources are permitted to load, thus mitigating risks like cross-site scripting (XSS) attacks. Similarly, headers like X-Content-Type-Options prevent browsers from interpreting files as a different type than what is intended, which helps in safeguarding against certain types of attacks. This functionality is essential for enforcing security measures directly through the browser, which helps in protecting both the server and the end-user from various vulnerabilities. Hence, security headers effectively inform the browser regarding actions to take with the site content, allowing for a more secure user experience. In contrast, while encrypting data transferred is a critical aspect of security, it is typically managed by Transport Layer Security (TLS) rather than through headers. Authentication of users is handled through other mechanisms such as tokens or cookies, rather than security headers. Furthermore, performance optimization relates to the efficiency of resource loading and is typically addressed through caching strategies or content delivery networks, not specifically

6. Which protocol does AWS IoT Core support for device connectivity?

A. HTTP/2

B. MQTT

C. WebSocket

D. FTP

AWS IoT Core primarily supports MQTT (Message Queuing Telemetry Transport) as its protocol for device connectivity. MQTT is specifically designed for low-bandwidth, high-latency, or unreliable networks and is highly efficient for remote device communication. It operates on a publish/subscribe model, allowing devices to easily send messages to the cloud and receive messages without needing to establish a direct connection continuously. This makes it particularly well-suited for IoT applications, where devices may be intermittently connected. While AWS IoT Core also supports other protocols such as HTTP and WebSocket for certain use cases, MQTT remains the dominant choice when it comes to facilitating effective, scalable communication for IoT devices. Its lightweight nature and ability to maintain persistent connections with lower overhead requirements make it ideal for the types of interactions and volume of messages typical in IoT environments.

7. Which of the following is a risk associated with not applying security patches promptly?

A. Increased operational costs

B. Higher chances of system outages

C. Exposure to vulnerabilities and exploits

D. Loss of hardware efficiency

The identification of exposure to vulnerabilities and exploits as a primary risk associated with not applying security patches promptly is vital for maintaining the integrity and security of any system. Security patches are designed to address known vulnerabilities in software that could be exploited by malicious actors. If these patches are not applied in a timely manner, the system remains susceptible to attacks, leading to potential data breaches, unauthorized access, or even total system compromise. By delaying or neglecting updates, organizations leave themselves open to threats that exploit these unaddressed vulnerabilities, increasing the likelihood of cyber incidents. This risk can have severe implications, including data loss, financial consequences, reputational damage, and regulatory penalties, making timely application of security patches critical in any security strategy. The other factors mentioned, while they might arise as secondary consequences of allowing vulnerabilities to exist, do not directly reflect the primary risk of enhancing exposure to potential exploits in the immediate context of cybersecurity.

8. Amazon Cognito serves as what type of service within AWS?

A. Data processing service

B. User directory and authentication server

C. Cloud storage solution

D. Serverless compute service

Amazon Cognito functions as a user directory and authentication server within AWS. This service is specifically designed to help developers manage user sign-ups, sign-ins, and access control processes seamlessly and securely. By acting as an authentication layer, Cognito allows applications to securely handle user information and identity management without requiring developers to build and maintain their own authentication systems. Cognito offers features such as user pools for managing user accounts and identity pools for granting access to AWS resources. This makes it particularly valuable in scenarios where applications require user authentication while still supporting various authentication methods, including social identity providers (like Google and Facebook) and enterprise identity providers through SAML. The other options reflect different AWS functionalities that do not match the core purpose of Amazon Cognito, reinforcing why the correct answer centers on its role as a user directory and authentication server.

9. Which AWS service can be used to monitor API calls?

A. AWS CloudTrail

B. AWS Config

C. AWS Shield

D. AWS Inspector

AWS CloudTrail is the service specifically designed for monitoring API calls made within your AWS account. It records account activity and API usage across your AWS infrastructure, enabling you to track changes, identify usage patterns, and audit access to resources. CloudTrail captures detailed information about API requests, including the identity of the requester, the time of the request, the source IP address, and the actions taken. This capability is crucial for security auditing, compliance reporting, and governance, as it allows organizations to understand who is doing what in their AWS environment. The other services mentioned focus on different aspects of AWS management and security. AWS Config is primarily used for monitoring configuration changes and compliance with rules, rather than API call tracking. AWS Shield provides DDoS protection and is not concerned with monitoring API activity. AWS Inspector is a security assessment service that reviews the configuration of AWS resources and identifies potential vulnerabilities, rather than tracking API interactions. Thus, the role of monitoring API calls distinctly aligns with the functionality of AWS CloudTrail.

10. Which service extracts, transforms, and delivers streaming data to various data stores and analytics services?

A. Amazon S3 Transfer Acceleration

B. Amazon Kinesis Data Firehose

C. AWS Direct Connect

D. AWS Data Pipeline

Amazon Kinesis Data Firehose is a fully managed service designed to easily load streaming data into data lakes, analytics services, and other data stores. This service offers capabilities to capture, transform, and load streaming data in real-time, allowing businesses to process and analyze their data without the need for heavy lifting related to infrastructure management. Kinesis Data Firehose can automatically scale to match the throughput of your data streams and seamlessly integrates with other AWS services like Amazon S3, Amazon Redshift, and Amazon Elasticsearch Service. Additionally, it supports transforming data on the fly using AWS Lambda, making it highly flexible for various use cases involving streaming data. The other services mentioned do have valuable functionalities, but they do not focus on the specific task of extracting, transforming, and delivering streaming data in the same way. For instance, Amazon S3 Transfer Acceleration is designed to speed up the upload of files to S3 but doesn't handle streaming data. AWS Direct Connect provides dedicated network connections from on-premises data centers to AWS but does not concern itself with data processing or transformation. AWS Data Pipeline is used for batch processing of data and managing workflows, rather than real-time streaming data.

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://awscertifiedsecurityspecialty.examzify.com

We wish you the very best on your exam journey. You've got this!