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

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

This is a sample study guide. To access the full version with hundreds of questions,

Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.

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. Don't worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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 type of record does CloudTrail event history provide?

A. Live performance metrics

B. Historical records of the last 90 days of events

C. Real-time system logs

D. Audit reports for user access

2. Which service would you use for real-time threat detection in AWS?

A. Amazon CloudTrail

B. Amazon GuardDuty

C. Amazon Inspector

D. AWS Config

3. What does AWS Config help you to achieve?

A. Consolidation of multiple accounts

B. Monitoring of application performance

C. Detailed views of AWS resource configurations

D. Management of data transfer

4. What type of network does Amazon VPC provide?

A. A virtual network dedicated to an AWS account

B. A global content delivery network

C. A shared internet connection

D. A multi-tenant cloud environment

5. What is the primary function of AWS Security Hub?

A. To monitor resource usage in real time

B. To aggregate security alerts from AWS services

C. To calculate resource costs

D. To automate deployment processes

6. What is the purpose of a Vault Lock policy in AWS?

A. To simplify instance launch

B. To restrict access to a vault

C. To manage AWS resources

D. To monitor network traffic

7. What is the purpose of AWS Trusted Advisor?

A. To monitor application performance

B. To provide insights into resource optimization

C. To consolidate multiple AWS accounts

D. To manage AWS resources through a command line

8. How does Amazon GuardDuty enhance security?

A. By providing threat detection and continuous monitoring of AWS accounts and workloads

B. By automating security compliance checks

C. By managing user access for AWS resources

D. By encrypting data at rest and in transit

9. What is the primary benefit of using Amazon GuardDuty?

A. It simplifies billing for multiple accounts

B. It provides efficient load balancing for applications

C. It offers continuous monitoring for malicious activity and anomalous behavior

D. It reduces costs by optimizing storage

10. How can you secure instances located in a public subnet?

A. By using AWS VPN

B. By utilizing security groups and network ACLs

C. By restricting access to a private subnet only

D. By turning off all ports

Answers

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

Explanations

1. What type of record does CloudTrail event history provide?

A. Live performance metrics

B. Historical records of the last 90 days of events

C. Real-time system logs

D. Audit reports for user access

CloudTrail event history provides historical records of the last 90 days of events, which is essential for monitoring user activity and API usage within an AWS account. This feature allows administrators to review actions taken on the AWS environment, enhancing security and compliance by providing insights into resource usage, changes made to configurations, and user access patterns. The ability to access event history for the past 90 days allows teams to investigate and analyze historical data without the need for persistent logging setup beyond this time frame. This can be critical in identifying unauthorized access attempts or changes made to critical resources that need to be tracked for security purposes. Other options either pertain to different functionalities such as performance metrics or logs which are not specific to the event history offered by CloudTrail. Audit reports and real-time logging, while important, do not specifically denote the nature of the historical recordings that CloudTrail provides, which are indeed focused on the last 90 days of API activity.

2. Which service would you use for real-time threat detection in AWS?

A. Amazon CloudTrail

B. Amazon GuardDuty

C. Amazon Inspector

D. AWS Config

Amazon GuardDuty is the service designed specifically for real-time threat detection in AWS environments. It continuously monitors for malicious or unauthorized behavior by analyzing data from various sources like AWS CloudTrail event logs, VPC Flow Logs, and DNS logs. GuardDuty uses machine learning, anomaly detection, and threat intelligence to identify potential security threats, allowing users to respond quickly to protect their AWS resources. This proactive approach is essential for maintaining a secure environment, and the alerts generated by GuardDuty can help security teams investigate and respond to issues before they have a significant impact. By using this service, organizations can strengthen their security posture by gaining insights into their AWS accounts and workloads in real time. In contrast, while other services like CloudTrail and AWS Config provide valuable information related to resource activities and compliance configuration, they are not specifically focused on real-time threat detection. Amazon Inspector, on the other hand, is a vulnerability assessment service used to identify security issues in applications but does not offer the same level of continuous threat monitoring as GuardDuty.

3. What does AWS Config help you to achieve?

A. Consolidation of multiple accounts

B. Monitoring of application performance

C. Detailed views of AWS resource configurations

D. Management of data transfer

AWS Config is a service that provides detailed views of AWS resource configurations, enabling users to assess how resource configurations comply with desired configurations. With AWS Config, you can track changes to configurations over time and understand the relationships between resources. This helps in auditing, compliance, and security management by ensuring that resources are compliant with policies and best practices. The ability to deliver a comprehensive history of resource configurations allows you to analyze misconfigurations, set up alerts for changes, and review the compliance of various resources against established standards. It provides a powerful tool for governance in a cloud environment by enabling visibility into resource setup and interactions. In contrast, consolidating multiple accounts involves using AWS Organizations and other services, which is not a feature of AWS Config. Monitoring application performance is primarily handled by services such as Amazon CloudWatch, which focuses on performance metrics rather than configuration states. Management of data transfer also falls outside the scope of AWS Config, as it pertains more to networking services like AWS Direct Connect or Amazon Transfer Family, rather than the monitoring of resource configurations.

4. What type of network does Amazon VPC provide?

A. A virtual network dedicated to an AWS account

B. A global content delivery network

C. A shared internet connection

D. A multi-tenant cloud environment

Amazon VPC provides a virtual private cloud that is dedicated to a single AWS account, allowing users to create isolated network environments within the AWS infrastructure. This enables organizations to have complete control over their networking resources, including the selection of IP address ranges, the creation of subnets, and the configuration of route tables and network gateways. A key benefit of using a virtual network dedicated to a specific AWS account is that it enhances security and privacy since resources within the VPC are not accessible to other AWS accounts or external networks unless explicitly configured. This isolation is critical for compliance and security-sensitive applications. Additionally, you can set up security groups and network ACLs to control inbound and outbound traffic at both the instance and subnet levels. The other options refer to different forms of networking or environments. A global content delivery network focuses on distributing content efficiently across geographical locations and is not specific to a virtual network for an AWS account. A shared internet connection implies a level of resource sharing that does not align with the private nature of a VPC. A multi-tenant cloud environment suggests that resources are shared among multiple customers, which contrasts with the dedicated aspect of an Amazon VPC.

5. What is the primary function of AWS Security Hub?

A. To monitor resource usage in real time

B. To aggregate security alerts from AWS services

C. To calculate resource costs

D. To automate deployment processes

The primary function of AWS Security Hub is to aggregate security alerts from various AWS services, providing a centralized view of security findings across an entire AWS environment. This service allows organizations to efficiently manage security at scale by collecting and prioritizing alerts generated by other AWS security services like Amazon GuardDuty, AWS Inspector, and AWS Firewall Manager. By consolidating security data, Security Hub enables security teams to quickly identify potential threats, vulnerabilities, and compliance issues, facilitating a more effective and timely response to incidents. This aggregation not only improves visibility but also aids in maintaining a strong security posture by allowing teams to assess the overall security findings and take necessary action on them. This function distinguishes AWS Security Hub as a crucial tool for organizations looking to enhance their security operations and ensure comprehensive oversight of their cloud infrastructure.

6. What is the purpose of a Vault Lock policy in AWS?

A. To simplify instance launch

B. To restrict access to a vault

C. To manage AWS resources

D. To monitor network traffic

The purpose of a Vault Lock policy in AWS is to restrict access to a vault. Vault Lock is a feature of AWS Glacier that allows users to enforce specific policies that govern how data in the vault can be accessed or modified. By locking down a vault, you ensure that certain access policies cannot be altered, thereby securing the contents against unauthorized access or accidental deletion. Implementing Vault Lock policies is particularly important for compliance purposes, as they help organizations ensure that the data retention and deletion rules are adhered to over time. Once a Vault Lock policy is set, it cannot be changed or removed, which adds a layer of protection for sensitive data stored in AWS Glacier. The other options relate to different functionalities in AWS or are not directly associated with the core purpose of Vault Lock. For instance, simplifying instance launch pertains to EC2 configurations, managing AWS resources involves broader services than just the vault, and monitoring network traffic relates to security services like AWS VPC Flow Logs or AWS GuardDuty rather than data vaulting.

7. What is the purpose of AWS Trusted Advisor?

A. To monitor application performance

B. To provide insights into resource optimization

C. To consolidate multiple AWS accounts

D. To manage AWS resources through a command line

AWS Trusted Advisor is a service designed to provide insights into resource optimization. Its primary purpose is to analyze your AWS environment and offer recommendations for improving performance, security, fault tolerance, and cost management. This includes identifying underutilized or idle resources that can be downsized or terminated to save costs and suggesting ways to optimize your existing architecture for better performance and efficiency. By leveraging Trusted Advisor, users can obtain actionable insights that align with best practices and optimize their AWS resources. This capability helps organizations to not only reduce unnecessary expenditures but also enhance the overall utilization of their cloud environment, resulting in better management of their AWS infrastructure. In this context, other choices do not directly align with the core functionality of AWS Trusted Advisor. Monitoring application performance is usually addressed by services like Amazon CloudWatch. Consolidating multiple AWS accounts doesn't reflect the cost optimization focus of Trusted Advisor and falls more under AWS Organizations and Control Tower. Managing AWS resources through a command line is typically handled by the AWS Command Line Interface (CLI), which is fundamentally different from the advisory role of Trusted Advisor.

8. How does Amazon GuardDuty enhance security?

A. By providing threat detection and continuous monitoring of AWS accounts and workloads

B. By automating security compliance checks

C. By managing user access for AWS resources

D. By encrypting data at rest and in transit

Amazon GuardDuty enhances security primarily through its capability for threat detection and continuous monitoring of AWS accounts and workloads. This service utilizes machine learning, anomaly detection, and integrated threat intelligence to identify potentially malicious activity and unauthorized behavior within an AWS environment. By continuously analyzing data from various sources, including AWS CloudTrail event logs, Amazon VPC Flow Logs, and DNS logs, GuardDuty can detect threats like account compromise, unusual API usage, and reconnaissance activity. Once a threat is identified, it generates findings which can alert administrators, allowing them to respond quickly to potential issues. This proactive monitoring mechanism is vital for maintaining a strong security posture and ensuring that any threats are promptly addressed before they can lead to significant damage or data breaches. The other options focus on different aspects of security management, such as compliance checks, user access management, and data encryption, which, while important, are not the core function of GuardDuty itself. GuardDuty is specifically designed for threat detection and monitoring, making that feature critical to its role in enhancing AWS security.

9. What is the primary benefit of using Amazon GuardDuty?

- A. It simplifies billing for multiple accounts
- B. It provides efficient load balancing for applications
- C. It offers continuous monitoring for malicious activity and anomalous behavior
- D. It reduces costs by optimizing storage

The primary benefit of using Amazon GuardDuty lies in its capability to offer continuous monitoring for malicious activity and anomalous behavior. GuardDuty is a threat detection service that utilizes machine learning, anomaly detection, and integrated threat intelligence to identify potential security threats across your AWS accounts, workloads, and data stored in AWS. By continuously analyzing accounts, VPC flow logs, AWS CloudTrail event logs, and DNS logs, GuardDuty can detect unauthorized access attempts, reconnaissance activities, and other suspicious behaviors in real time. This proactive security measure enables organizations to respond quickly to potential threats, thereby enhancing their overall security posture. The other options do not align with the primary function of GuardDuty. Simplifying billing pertains more to AWS Organizations features rather than a specific security tool. Load balancing is handled by services such as Elastic Load Balancing, not GuardDuty. Lastly, while cost optimization can be a significant factor in AWS management, it falls under different service categories focused on storage and budget management, not on the critical security surveillance that GuardDuty provides.

10. How can you secure instances located in a public subnet?

- A. By using AWS VPN
- B. By utilizing security groups and network ACLs
- C. By restricting access to a private subnet only
- D. By turning off all ports

Utilizing security groups and network ACLs is the most effective way to secure instances located in a public subnet. Security groups act as virtual firewalls for your instances, allowing you to define inbound and outbound rules based on IP protocols, ports, and source/destination IP addresses. This granular control enables you to limit traffic to only what is necessary, thereby reducing the attack surface of your instances. Network ACLs, on the other hand, provide an additional layer of security at the subnet level. They operate as stateless firewalls that can control traffic in both directions, allowing or denying traffic based on defined rules. By effectively configuring both security groups and network ACLs, you can ensure that only authorized traffic reaches your public instances. In comparison, other options, while they might enhance security in different contexts, do not directly address how to secure instances specifically within a public subnet. For instance, simply using a VPN does not provide protection for public instances and mainly focuses on creating secure connections for accessing the network. Restricting access strictly to a private subnet may isolate instances, but it doesn't directly apply to securing public instances. Turning off all ports may seem secure, but it would also effectively make the instances inaccessible for legitimate use. Thus, the combination of security

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!