SECURITY IN AMAZON WEB SERVICES (CISN 74A) PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://securityinaws.examzify.com

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. How is a security group defined in AWS?

A. A virtual network for AWS services

B. A type of AWS storage solution

C. A virtual firewall for EC2 instances

D. A configuration management tool for resources

2. Who is responsible for operating, managing, and controlling security OF the cloud in the shared responsibility model?

A. AWS

B. Customers

C. Third-party vendors

D. Partners

3. What is the purpose of AWS Firewall Manager?

A. To handle data transfers outside AWS

B. To manage IAM policies centrally

C. To configure and manage firewall rules across AWS Organization

D. To track changes in AWS resources

4. What kind of information can be extracted from server access logs regarding the date and time of events?

A. The frequency of access attempts

B. The duration of user sessions

C. The exact timing of resource interactions

D. The location of users

5. What is a key characteristic of the security principle to prepare for security events?

A. Implementing firewall rules

B. Routinely practicing incident response through game days

C. Restricting access rights

D. Conducting vulnerability assessments

6. How can security automation be achieved in AWS?

A. By using manual testing procedures

B. By using AWS Lambda or AWS Step Functions for automation

C. By hiring a dedicated security team

D. By keeping security checks entirely offline

7. Which of these responsibilities is NOT part of the customer's role in AWS security?

A. Patching network infrastructure

B. Managing customer data

C. Managing account credentials

D. Implementing data encryption

8. Which security feature allows for stateful control of traffic to and from Amazon EC2 instances?

A. NAT gateway

B. Security groups

C. Route tables

D. Network ACLs

9. What is a primary function of AWS Shield?

A. To protect against DDoS attacks

B. To manage IAM user permissions

C. To monitor financial costs of services

D. To perform security assessments of applications

10. What are the benefits of using AWS Security Token Service (STS)?

A. It allows for the permanent access of AWS services

B. It enables you to grant temporary, limited-access credentials for AWS services

C. It provides data encryption for AWS resources

D. It monitors network traffic for malicious activity

Answers

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

Explanations

1. How is a security group defined in AWS?

A. A virtual network for AWS services

B. A type of AWS storage solution

C. A virtual firewall for EC2 instances

D. A configuration management tool for resources

A security group in AWS is defined as a virtual firewall for Amazon Elastic Compute Cloud (EC2) instances. This definition highlights its primary role in controlling inbound and outbound traffic to instances within a Virtual Private Cloud (VPC). When you create a security group, you specify rules that allow or deny traffic based on protocols, ports, and source or destination IP address ranges. Each EC2 instance can be associated with one or more security groups, enabling fine-grained control over network access. The default behavior of a security group is to deny all inbound traffic and allow all outbound traffic unless rules are explicitly defined. This functionality is crucial for maintaining the security posture of applications and services hosted on AWS. By managing access at the instance level, organizations can implement layered security measures, which are fundamental for protecting sensitive data and resources in the cloud. In contrast, the other options do not accurately describe a security group's purpose or functionality within the AWS ecosystem. For example, while a virtual network relates to broader network configurations in AWS, it does not pertain specifically to the function of security groups. Similarly, AWS storage solutions and configuration management tools serve different operational roles, unrelated to the specific task of controlling network traffic for EC2 instances.

2. Who is responsible for operating, managing, and controlling security OF the cloud in the shared responsibility model?

A. AWS

B. Customers

C. Third-party vendors

D. Partners

In the context of the shared responsibility model in AWS, the responsibility for operating, managing, and controlling security OF the cloud falls to AWS. This means that AWS is tasked with ensuring the security of the physical infrastructure, networking, and hypervisor that make up its cloud services. AWS invests in various security measures, compliance certifications, and robust operational processes to protect its environment from threats, maintain data sovereignty, and ensure service availability. This model delineates boundaries where AWS maintains control over the underlying infrastructure and hardware layers, handling vulnerabilities and threats that could affect these core components. Customers, on the other hand, are responsible for managing security IN the cloud, which includes access management, data encryption, and compliance for the applications and data they deploy. Understanding this division of responsibilities is crucial, as it helps customers recognize where their duties begin and AWS's responsibilities end, promoting a secure cloud utilization strategy.

3. What is the purpose of AWS Firewall Manager?

A. To handle data transfers outside AWS

B. To manage IAM policies centrally

C. To configure and manage firewall rules across AWS Organization

D. To track changes in AWS resources

AWS Firewall Manager is specifically designed to help organizations centrally configure and manage firewall rules across their AWS environment. This service is extremely beneficial for enterprises that operate multiple accounts within an AWS Organization, as it provides a consistent and streamlined approach to security management. With Firewall Manager, security administrators can create rules for AWS WAF (Web Application Firewall), manage security policies, and ensure compliance across all accounts and resources, making security governance much simpler. This capability helps prevent security misconfigurations that may arise when policies are applied inconsistently across different accounts. By utilizing AWS Firewall Manager, organizations enhance their overall security posture by ensuring that the same rules are enforced everywhere within the AWS ecosystem. This central management not only saves time but also reduces the risk of vulnerabilities arising from misalignment in firewall settings across various accounts.

4. What kind of information can be extracted from server access logs regarding the date and time of events?

A. The frequency of access attempts

B. The duration of user sessions

C. The exact timing of resource interactions

D. The location of users

Server access logs provide detailed records of interactions with a server, capturing specific events and activities. Among the crucial pieces of information logged are the timestamps that indicate when each event occurred. This enables the identification of the exact timing of resource interactions. Having precise timestamps is vital for various purposes, such as troubleshooting issues, analyzing traffic patterns, and conducting security audits. The timestamps allow administrators and security analysts to track user interactions, establish timelines of events, and correlate logs for incident response. Other aspects, while significant, focus on different types of analysis. For instance, frequency of access attempts relates to how often users or systems interact with the server but does not provide exact timing for individual interactions. Similarly, duration of user sessions indicates how long a user was connected but again lacks the specificity of when those sessions started or ended. User location tracking is useful for understanding geographical usage patterns but does not address the timing of specific resource interactions.

5. What is a key characteristic of the security principle to prepare for security events?

A. Implementing firewall rules

B. Routinely practicing incident response through game days

C. Restricting access rights

D. Conducting vulnerability assessments

Routinely practicing incident response through game days is a key characteristic of the security principle focused on preparing for security events. This practice allows organizations to simulate real-life security incidents and test their response strategies without the pressures of an actual event. Game days help teams understand their roles, improve communication, and identify gaps in their processes or tools. By providing a controlled environment for practice, the organization can refine its incident response plan, ensuring that staff are well-prepared to act swiftly and effectively in the event of a security breach or incident. In contrast, implementing firewall rules, restricting access rights, and conducting vulnerability assessments are important components of a security strategy but are typically more focused on prevention, access control, and proactive threat identification rather than the specific preparation for responding to security incidents. While each of these elements contributes to an overall security posture, they do not specifically emphasize the critical aspect of readiness to respond effectively when an event occurs, making the practice of incident response through game days the most fitting choice for this question.

6. How can security automation be achieved in AWS?

A. By using manual testing procedures

B. By using AWS Lambda or AWS Step Functions for automation

C. By hiring a dedicated security team

D. By keeping security checks entirely offline

Security automation in AWS can be effectively achieved by utilizing services like AWS Lambda or AWS Step Functions. These services enable users to automate security tasks and processes without the need for manual intervention, resulting in a more efficient and reliable security posture. AWS Lambda allows you to run code in response to events, making it a powerful tool for automating security responses, such as incident response workflows or automatic remediation. For instance, if a security threat is detected, Lambda can trigger an automated function to isolate an affected instance or notify administrators, streamlining the response time and reducing potential damage. AWS Step Functions further enhance this automation by enabling the orchestration of multiple AWS services into serverless workflows. These workflows can include a series of security checks, validations, or actions, allowing for complex security automation scenarios that can be easily managed and scaled. In contrast, relying on manual testing procedures would slow down the response to security threats and may lead to inconsistencies. Hiring a dedicated security team, while beneficial, does not automate the security processes themselves, and keeping security checks offline would hinder the ability to respond quickly to threats, especially in the cloud context where immediate action is often needed. Therefore, leveraging AWS Lambda or AWS Step Functions provides an effective means of achieving security automation, addressing vulnerabilities

7. Which of these responsibilities is NOT part of the customer's role in AWS security?

A. Patching network infrastructure

B. Managing customer data

C. Managing account credentials

D. Implementing data encryption

In the shared responsibility model of AWS, security is divided between AWS and the customer. AWS is responsible for the security of the cloud infrastructure itself, which includes the physical hardware, the storage, and the networking components that make up the services. The customer, on the other hand, is responsible for anything that they deploy or manage within those services. Patching network infrastructure is a responsibility that lies primarily with AWS. They manage the physical and virtual components of the networking stack and ensure that it is up to date and secure. The customer, however, must manage other aspects of security, which include managing customer data, controlling account credentials, and implementing data encryption. These responsibilities are crucial for maintaining the security and integrity of applications and data hosted on AWS. Thus, the correct response highlights the unique role of AWS in maintaining the foundational security of its services while delineating the specific security responsibilities that fall to the customer.

8. Which security feature allows for stateful control of traffic to and from Amazon EC2 instances?

A. NAT gateway

B. Security groups

C. Route tables

D. Network ACLs

Stateful control of traffic to and from Amazon EC2 instances is achieved through security groups. Security groups act as virtual firewalls for your EC2 instances, controlling both inbound and outbound traffic. They enable you to define specific rules that allow or deny traffic based on IP addresses, protocols, and port numbers. The key characteristic of security groups is their stateful nature; if an inbound request is allowed, the response to that request is automatically permitted, regardless of the outbound rules. This means that once a connection is established, the subsequent traffic from the response is allowed through without needing separate rules. In contrast, features like NAT gateways, route tables, and network ACLs do not offer the same level of stateful management for traffic. NAT gateways primarily enable instances in a private subnet to connect to the internet, while route tables determine the traffic routing within VPC. Network ACLs, on the other hand, provide stateless filtering and impose rules for inbound and outbound traffic, requiring separate rules for each direction, which can be less intuitive than security groups' stateful approach.

9. What is a primary function of AWS Shield?

A. To protect against DDoS attacks

B. To manage IAM user permissions

C. To monitor financial costs of services

D. To perform security assessments of applications

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service designed to safeguard applications running on AWS. Its primary function is to provide automatic detection and mitigation against DDoS attacks, ensuring that applications remain available and performant even when under attack. Shield offers two tiers of service: Shield Standard, which is automatically included at no additional cost for all AWS customers, providing protection against the most common and frequently occurring attacks, and Shield Advanced, which offers enhanced protections, additional features, and support for complex attacks. The other options focus on different aspects of AWS services. Managing IAM user permissions relates to AWS Identity and Access Management (IAM), monitoring financial costs concerns services like AWS Cost Explorer, and security assessments of applications are typically performed using services like AWS Inspector. Each of these areas is vital for a comprehensive security strategy, but none address the specific function of AWS Shield in protecting against DDoS attacks.

10. What are the benefits of using AWS Security Token Service (STS)?

A. It allows for the permanent access of AWS services

B. It enables you to grant temporary, limited-access credentials for AWS services

C. It provides data encryption for AWS resources

D. It monitors network traffic for malicious activity

Using AWS Security Token Service (STS) provides several essential benefits that enhance security and flexibility when managing access to AWS resources. The key advantage is its ability to grant temporary, limited-access credentials for AWS services. This capability significantly reduces the risk associated with long-term credentials. By issuing temporary credentials, STS allows for a more secure access mechanism. These credentials are typically granted for short durations, minimizing exposure in case they are compromised. Since they are temporary, users do not have constant access to resources, which aligns with the principle of least privilege—granting only the permissions necessary for a specific task, and only for a limited time. This is especially beneficial for applications and users who require access to AWS services for a short period or specific operations without the need for long-term credentials. Furthermore, STS can be integrated with various identity providers and can be utilized in scenarios involving federated authentication, which makes it ideal for organizations that manage access for multiple users and systems securely. The other options focus on permanent access, data encryption, and network traffic monitoring, which are not the core functions of AWS STS. While they are important security considerations within AWS, they do not reflect the primary function and benefits provided by AWS Security Token Service.

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://securityinaws.examzify.com

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