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

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

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

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. How does AWS ensure data integrity in cloud services?

A. By using manual audits

B. By maintaining comprehensive data logs and version histories

C. By solely relying on customer certificates

D. By backing up data every six months

2. Which of the following is a recommended best practice for network protection?

A. Allow unrestricted inbound traffic

B. Use security groups to control access to resources

C. Isolate all resources in public subnets

D. Disable VPC Flow logs

3. Which option is considered a best practice for configuring long-term access in AWS IAM?

A. Attach IAM policies to individual users for better tracking.

B. Attach IAM policies to IAM groups and assign users to those groups.

C. Create a single IAM user for all team members.

D. Only use AWS Managed Policies without customization.

4. What does AWS CloudTrail provide insight into?

A. Resource utilization and performance metrics

B. Network traffic patterns

C. User activity and API usage across AWS resources

D. Automated backup solutions

5. What does Multi-Factor Authentication (MFA) provide in AWS?

A. A single point of access for user management

B. An additional layer of security for accounts

C. A method for managing billing and cost

D. Enhanced user interface customization options

SAMPLE

6. How can accidental deletion of critical AWS resources be prevented?

A. By enabling multi-factor authentication for all users

B. By enabling resource policies and using AWS Resource Access Manager

C. By regularly backing up data to Amazon S3

D. By using AWS Config to monitor resource changes

7. Which AWS service relies on user pools and identity pools?

A. Amazon Cognito.

B. AWS Identity Store.

C. AWS IAM Console.

D. Amazon API Gateway.

8. 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

9. Which service helps automate patch deployments in AWS?

A. AWS CloudFormation

B. AWS Systems Manager Patch Manager

C. AWS OpsWorks

D. AWS Elastic Beanstalk

10. What is the significance of using AWS Resource Access Manager?

A. To automatically deploy resources in multiple regions

B. To share resources securely across accounts

C. To monitor API calls made to resources

D. To create billing alerts for resource usage

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. How does AWS ensure data integrity in cloud services?

A. By using manual audits

B. By maintaining comprehensive data logs and version histories

C. By solely relying on customer certificates

D. By backing up data every six months

The correct answer highlights AWS's commitment to data integrity through the maintenance of comprehensive data logs and version histories. This approach allows AWS to track and verify changes made to data, ensuring that any unauthorized modifications or corruption can be detected and addressed promptly. The ability to refer back to previous versions of data also enables recovery from accidental deletions or unintended changes, which is fundamental in maintaining the overall integrity of the data stored in the cloud. Maintaining comprehensive logs can also aid in compliance with regulatory requirements and support auditing activities. This level of oversight contributes to the transparency and trustworthiness of the data management practices in AWS. Other options do not address data integrity as effectively. Manual audits can be helpful but are not a scalable or efficient method for ongoing data integrity checks. Relying solely on customer certificates does not inherently provide safeguards for the integrity of data itself, as certificates are primarily focused on authentication and encryption. Backing up data every six months is too infrequent to ensure data integrity, as it does not allow for immediate recovery or validation of data changes that may occur in-between backup sessions.

2. Which of the following is a recommended best practice for network protection?

A. Allow unrestricted inbound traffic

B. Use security groups to control access to resources

C. Isolate all resources in public subnets

D. Disable VPC Flow logs

Using security groups to control access to resources is a fundamental best practice for network protection in AWS. Security groups act as virtual firewalls for your AWS resources, such as EC2 instances, allowing you to define inbound and outbound traffic rules. By setting these rules, you can specify which IP addresses or ranges are allowed to connect and which ports they can use, thereby minimizing exposure to potential threats. This granular control helps to ensure that only authorized traffic can reach your resources, which is essential for maintaining the overall security posture of your infrastructure. Unlike options that suggest allowing unrestricted inbound traffic or isolating all resources in public subnets, which can significantly increase vulnerability, security groups provide a mechanism to limit access efficiently. Additionally, disabling VPC Flow logs would hinder your ability to monitor and audit traffic, making it difficult to detect unauthorized access or suspicious behavior. Thus, utilizing security groups is crucial for protecting network resources effectively.

SAMPLE

3. Which option is considered a best practice for configuring long-term access in AWS IAM?

A. Attach IAM policies to individual users for better tracking.

B. Attach IAM policies to IAM groups and assign users to those groups.

C. Create a single IAM user for all team members.

D. Only use AWS Managed Policies without customization.

Attaching IAM policies to IAM groups and assigning users to those groups is a recognized best practice for configuring long-term access in AWS Identity and Access Management (IAM). This approach streamlines permission management and enhances security by allowing for easier policy updates and consistency in permissions across users. When policies are attached to groups instead of individual users, it simplifies the process of managing permissions. For instance, if a new user joins the team, they can simply be added to the relevant group(s) which automatically grants them the permissions defined in those groups. This reduces the risk of errors that can occur when managing permissions on a per-user basis, as changes made to a group policy will propagate to all users within that group. Additionally, grouping users based on their roles or responsibilities aligns with the principle of least privilege. This means that users only receive the minimum necessary permissions they need to perform their job functions, thereby limiting potential security vulnerabilities. In summary, using IAM groups not only enhances manageability and organization but also importantly supports security best practices within AWS environments.

4. What does AWS CloudTrail provide insight into?

A. Resource utilization and performance metrics

B. Network traffic patterns

C. User activity and API usage across AWS resources

D. Automated backup solutions

AWS CloudTrail is a service that provides detailed logs of user activity and API usage across various AWS resources. It captures information such as who made changes, what actions were performed, and when these actions took place. This insight is crucial for organizations to maintain security, compliance, and operational auditing. By tracking the API calls made within an AWS account, CloudTrail helps administrators monitor user activity and detect anomalies or unauthorized actions. It also enables better incident response and forensic analysis by allowing users to trace back actions to specific users or roles. The other options focus on different aspects: resource utilization and performance metrics generally pertain to services like Amazon CloudWatch, which monitors operational health; network traffic patterns are monitored through services like VPC Flow Logs; and automated backup solutions are provided by services like AWS Backup or Elastic Block Store snapshots. None of these functionalities relate to the core purpose of CloudTrail, which centers on capturing and logging user activities and API interactions.

SAMPLE

5. What does Multi-Factor Authentication (MFA) provide in AWS?

A. A single point of access for user management

B. An additional layer of security for accounts

C. A method for managing billing and cost

D. Enhanced user interface customization options

Multi-Factor Authentication (MFA) in AWS provides an additional layer of security for accounts. By requiring more than one form of verification to access an account, MFA significantly enhances security beyond just a username and password. This extra step typically involves something the user knows (like a password) and something the user possesses (such as a mobile device generating a one-time code). In a security context, MFA is crucial because it helps to protect sensitive data and resources from unauthorized access. Even if a password is compromised, the account remains secure as long as the second factor—typically a time-sensitive code generated by an authenticator app or sent via SMS—is not also compromised. Therefore, its primary role in AWS is to fortify account security by ensuring that validation involves multiple credentials. The other options do not correctly reflect the primary purpose of MFA in AWS. User management or billing activities do not define its function, nor does it relate to user interface customization. MFA is specifically about securing account access through multiple forms of verification.

6. How can accidental deletion of critical AWS resources be prevented?

A. By enabling multi-factor authentication for all users

B. By enabling resource policies and using AWS Resource Access Manager

C. By regularly backing up data to Amazon S3

D. By using AWS Config to monitor resource changes

Preventing accidental deletion of critical AWS resources is best addressed by enabling resource policies and using AWS Resource Access Manager. Resource policies provide a way to define permissions at a granular level for specific resources, allowing you to control who can delete or modify them. By using these policies, organizations can enforce strict access controls, ensuring that only authorized users or roles have the ability to delete sensitive resources. Additionally, AWS Resource Access Manager allows for efficient sharing of AWS resources across accounts with clear ownership and resource controls, further enhancing security and reducing the risk of accidental deletions. By structuring permissions around users' needs and defining resource-specific policies, organizations can create a more secure environment that mitigates the risk of accidental deletions. While multi-factor authentication enhances the overall security posture and reduces the likelihood of unauthorized access, it does not specifically target the prevention of accidental deletions. Backing up data to Amazon S3 is crucial for data recovery but does not prevent deletion itself; rather, it is a recovery mechanism. Monitoring resource changes with AWS Config helps track changes to AWS resources but does not actively prevent accidental deletions from occurring. Hence, enabling resource policies in conjunction with resource access management is the most effective solution to avoid accidental deletions of critical resources.

SAMPLE

7. Which AWS service relies on user pools and identity pools?

A. Amazon Cognito.

B. AWS Identity Store.

C. AWS IAM Console.

D. Amazon API Gateway.

Amazon Cognito is the service that relies on user pools and identity pools to provide secure user authentication, authorization, and management. User pools in Amazon Cognito allow you to manage user registration, authentication, and account recovery. They enable you to create a user directory that can scale to millions of users, allowing for features such as multi-factor authentication and customizable workflows. Identity pools, on the other hand, provide access to AWS services for users, allowing for temporary, limited permissions using AWS credentials meant for accessing other AWS resources. This setup facilitates seamless integration of user authentication with authorization to access AWS services, making it easier to build scalable and secure applications. The distinction lies in user pools focusing on user management, while identity pools handle authorization to AWS resources, both of which are critical for developing secure applications in the AWS ecosystem. Other options like the AWS Identity Store, AWS IAM Console, and Amazon API Gateway do not utilize user pools and identity pools in the same way as Amazon Cognito does, as they serve different roles within the AWS security framework and service architecture.

8. 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.

SAMPLE

9. Which service helps automate patch deployments in AWS?

A. AWS CloudFormation

B. AWS Systems Manager Patch Manager

C. AWS OpsWorks

D. AWS Elastic Beanstalk

AWS Systems Manager Patch Manager is specifically designed to automate the process of patching managed instances in AWS. It enables users to automate the process of applying patches for both operating systems and applications, which is crucial for maintaining security and compliance. Patch Manager allows for the configuration of patch baselines, defining which patches should be applied and when, as well as automating the patching process across numerous instances, thereby saving time and minimizing manual effort involved in keeping systems up-to-date. This service is part of AWS Systems Manager, which provides operational data from multiple AWS services to automate tasks across AWS resources. By utilizing Patch Manager, AWS customers can ensure that their environments remain secure by regularly applying updates and vulnerabilities patches, which is a key aspect of any security strategy. The other options, while useful AWS services, do not specifically focus on the automation of patch deployments. AWS CloudFormation is primarily for infrastructure as code, allowing users to model and set up AWS resources. AWS OpsWorks is a configuration management service that can manage stacks and deploy applications but does not specialize in patch management. AWS Elastic Beanstalk simplifies application deployment but does not provide features specifically for managing patches across instances. Hence, Systems Manager Patch Manager stands out as the dedicated solution for automating patch deployments

10. What is the significance of using AWS Resource Access Manager?

A. To automatically deploy resources in multiple regions

B. To share resources securely across accounts

C. To monitor API calls made to resources

D. To create billing alerts for resource usage

Using AWS Resource Access Manager is significant for sharing resources securely across different AWS accounts. This functionality enables organizations to efficiently manage their resources by allowing certain resources, such as subnets, transit gateways, and license configurations, to be made available across multiple accounts without needing to duplicate those resources. By leveraging resource sharing, organizations can improve collaboration among teams and make better use of their infrastructure, leading to more efficient resource management. This capability also helps in maintaining a clear security model, as shared resources can be accessed under strict permissions, ensuring that only authorized accounts can utilize them. Such centralized control over resource access is crucial for maintaining security and oversight in multi-account environments. The other options pertain to functions that AWS provides but do not relate directly to the purpose of AWS Resource Access Manager. For example, deploying resources in multiple regions is accomplished through separate AWS services, monitoring API calls involves tools like AWS CloudTrail, and billing alerts are set up through AWS Budgets, none of which align with the core functionality of resource sharing that AWS Resource Access Manager facilitates.

SAMPLE

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!

SAMPLE