Security in Amazon Web Services (CISN 74A) 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. **Which AWS service can help manage encryption keys in compliance with regulation standards?**

   A. AWS IAM

   B. AWS CloudTrail

   C. AWS Key Management Service

   D. AWS WAF

2. **What does an internet gateway in a VPC do?**

   A. Provides load balancing for internal resources

   B. Acts as a target for internet-routable traffic

   C. Securely connects multiple VPCs

   D. Encrypts data in transit

3. **What type of actions does AWS CloudTrail record?**

   A. Only actions taken by administrators.

   B. All actions taken within your AWS Management Console, AWS CLI, and APIs.

   C. Only successful API calls.

   D. Actions that occur outside of AWS services.

4. **Which service logs would provide the MOST insight into how users are using a web application with EC2 instances behind a load balancer?**

   A. Amazon S3 access logs.

   B. Elastic Load Balancing (ELB) access logs.

   C. Amazon CloudWatch logs.

   D. AWS Lambda logs.

5. **Which AWS service uses NLP to classify sensitive data stored in AWS?**

   A. Amazon Transcribe

   B. Amazon Comprehend

   C. Amazon Macie

   D. AWS Lambda

6. 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.

7. Which statement about Amazon CloudWatch is true?

A. CloudWatch only monitors network traffic.

B. CloudWatch provides the ability to create alarms and sends notifications.

C. CloudWatch can only visualize data from EC2 instances.

D. CloudWatch is not useful for detecting anomalies.

8. 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

9. What does the term 'network address translation' (NAT) refer to?

A. A method for optimizing network performance

B. A technique for allowing multiple devices to share a single public IP

C. A way to encrypt data on a network

D. A process for segregating network traffic

10. What is the primary function of AWS IAM roles?

A. To manage AWS account billing and payment

B. To allow multiple users access to Amazon EC2 instances

C. To enable cross-account access and permissions delegation

D. To create VPCs and manage subnets

Answers

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

Explanations

1. Which AWS service can help manage encryption keys in compliance with regulation standards?

A. AWS IAM

B. AWS CloudTrail

C. AWS Key Management Service

D. AWS WAF

AWS Key Management Service (KMS) is specifically designed to help manage encryption keys, making it a robust solution for organizations that need to comply with various regulatory standards. KMS allows users to create, control, and manage cryptographic keys across AWS services and in their own applications. It simplifies the process of key management, ensuring that sensitive data is encrypted, while also allowing organizations to maintain compliance with standards such as PCI-DSS, HIPAA, and others. KMS provides features such as key policies, IAM policies, and grants to control access to keys, allowing for fine-grained permission models that meet regulatory requirements. The service also integrates with other AWS services to automate encryption processes, making it easier for users to adhere to compliance mandates. Additionally, KMS supports logging capabilities via AWS CloudTrail, which helps track the usage and management of keys, providing an audit trail necessary for compliance audits. In contrast, AWS IAM focuses on managing user access and permissions rather than on key management itself. AWS CloudTrail provides logging of API calls made on your account to help with auditing and compliance but does not manage encryption keys. AWS WAF is a web application firewall that helps protect applications from common web exploits and is not related to key management or compliance standards.

2. What does an internet gateway in a VPC do?

A. Provides load balancing for internal resources

B. Acts as a target for internet-routable traffic

C. Securely connects multiple VPCs

D. Encrypts data in transit

An internet gateway in a Virtual Private Cloud (VPC) primarily functions as a target for internet-routable traffic, which facilitates communication between resources within the VPC and the internet. By attaching an internet gateway to a VPC, you enable instances within that VPC to access the internet and for external users to reach those instances if they have public IP addresses. When an instance needs to communicate with the internet, the internet gateway will route the outbound traffic from that instance to the public internet. Similarly, it can handle incoming traffic from the internet to the instances, allowing for proper routing and addressing. This is essential for applications that need to be publicly accessible or that rely on internet-based services. The other options refer to functionalities that are not associated with an internet gateway. Load balancing pertains to evenly distributing network or application traffic across multiple servers, while connecting multiple VPCs securely generally involves using VPC peering or AWS Transit Gateway, rather than an internet gateway. Data encryption in transit typically falls under different services and techniques, such as using SSL/TLS protocols. Thus, option B accurately describes the role of an internet gateway in a VPC.

3. What type of actions does AWS CloudTrail record?

A. Only actions taken by administrators.

B. All actions taken within your AWS Management Console, AWS CLI, and APIs.

C. Only successful API calls.

D. Actions that occur outside of AWS services.

AWS CloudTrail records all actions taken within your AWS Management Console, AWS CLI, and APIs. This comprehensive logging capability enables users to capture a full history of AWS API calls, which includes information such as who made the call, the services that were accessed, and the actions that were performed. This functionality is crucial for auditing, compliance, and security analysis, as it provides insights into the activities and behaviors within your AWS environment. The ability to log all actions helps organizations track changes, troubleshoot issues, and respond to security incidents effectively. It contributes to a better understanding of resource usage and management practices. Thus, the correct answer encompasses the broad scope of actions that CloudTrail monitors, rather than limiting it to one specific type or subset of activities.

4. Which service logs would provide the MOST insight into how users are using a web application with EC2 instances behind a load balancer?

A. Amazon S3 access logs.

B. Elastic Load Balancing (ELB) access logs.

C. Amazon CloudWatch logs.

D. AWS Lambda logs.

Elastic Load Balancing (ELB) access logs provide detailed insights into how users interact with a web application that is utilizing EC2 instances behind a load balancer. These logs capture information about each request sent to the load balancer, including the request's source IP address, request processing time, backend response time, and response codes. This information is vital for understanding traffic patterns, identifying performance bottlenecks, troubleshooting errors, and optimizing application performance. The ELB access logs essentially serve as a complete record of the requests made to your load balancer, which can be analyzed to gain insights about user behavior, the types of requests being made, and how efficiently the EC2 instances are handling those requests. This logging is especially valuable for applications where high availability and traffic management are critical. While other logging services such as Amazon S3 access logs and Amazon CloudWatch logs provide useful information for certain use cases, they do not specifically focus on user interaction with the application in the context of load-balanced traffic. Amazon S3 access logs track requests made to S3 buckets, and CloudWatch logs primarily monitor system performance and resource utilization rather than capturing detailed request-level data. AWS Lambda logs pertain to functions run in response to events, which is not applicable in

5. Which AWS service uses NLP to classify sensitive data stored in AWS?

A. Amazon Transcribe

B. Amazon Comprehend

C. Amazon Macie

D. AWS Lambda

Amazon Macie is specifically designed to help identify and classify sensitive data within AWS environments, such as personally identifiable information (PII) and intellectual property. It utilizes machine learning and natural language processing (NLP) to automatically discover and classify data stored in services like Amazon S3, helping organizations enforce data security policies and manage compliance requirements effectively. By leveraging NLP, Amazon Macie can analyze the content of the stored data and identify potential security risks, allowing businesses to take proactive measures to protect sensitive information. This capability is essential for organizations that need to comply with regulatory standards and ensure that sensitive data is handled appropriately. The other options, while valuable AWS services, focus on different functionalities. For instance, Amazon Transcribe provides speech-to-text capabilities, Amazon Comprehend is primarily used for text analysis and sentiment detection, and AWS Lambda is a serverless compute service that executes code in response to certain triggers, rather than specifically focusing on data classification.

6. 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.

7. Which statement about Amazon CloudWatch is true?

A. CloudWatch only monitors network traffic.

B. CloudWatch provides the ability to create alarms and sends notifications.

C. CloudWatch can only visualize data from EC2 instances.

D. CloudWatch is not useful for detecting anomalies.

Amazon CloudWatch plays a critical role in monitoring and management within Amazon Web Services. The statement that CloudWatch provides the ability to create alarms and sends notifications highlights one of its significant functionalities. With CloudWatch, users can set up alarms based on metrics—such as CPU utilization, disk reads/writes, and network traffic—allowing for proactive management of resources. When a specified threshold is breached, CloudWatch can automatically trigger notifications to alert administrators or take defined actions like scaling resources or stopping an instance. This capability is essential for maintaining system health, optimizing resource usage, and ensuring reliability. The other statements present limitations that do not accurately reflect the comprehensive features of CloudWatch, such as its ability to monitor a wide range of AWS services, not just network traffic, and visualize data from various sources beyond EC2 instances. Additionally, CloudWatch can help detect anomalies through its monitoring capabilities, which is contrary to any suggestion that it is not useful for that purpose.

8. 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.

9. What does the term 'network address translation' (NAT) refer to?

A. A method for optimizing network performance

B. A technique for allowing multiple devices to share a single public IP

C. A way to encrypt data on a network

D. A process for segregating network traffic

Network Address Translation (NAT) is primarily a technique that allows multiple devices on a local network to share a single public IP address for accessing external networks, such as the internet. This process is essential for conserving the number of public IP addresses used, as there are limited numbers available. When a device within a private network initiates a request to an external network, NAT replaces the private IP address of the device with the public IP address, allowing the response to be accurately routed back to the requesting device. This capability supports various devices, such as computers, smartphones, and smart home devices, facilitating their ability to communicate with external web services while maintaining a layer of obscurity and internal network organization. Additionally, it enhances security since devices are not directly exposed to the internet but rather communicate through the NAT router. Understanding this function allows one to appreciate how NAT plays a vital role in network management, as well as its implications for security and the limitations it may impose on certain types of traffic, such as peer-to-peer services or applications that require inbound connections.

10. What is the primary function of AWS IAM roles?

A. To manage AWS account billing and payment

B. To allow multiple users access to Amazon EC2 instances

C. To enable cross-account access and permissions delegation

D. To create VPCs and manage subnets

The primary function of AWS Identity and Access Management (IAM) roles is to enable cross-account access and permissions delegation. IAM roles are designed to provide secure access to AWS resources without the need to share long-term credentials. They can be assumed by users, applications, or AWS services, allowing these entities to interact with other AWS resources as needed based on the permissions assigned to the role. Using IAM roles facilitates scenarios such as granting temporary credentials for users from another AWS account or allowing an application running on an Amazon EC2 instance to access resources in another account. This enhances the security model because it reduces the risk associated with distributing permanent credentials. By working with IAM roles, organizations can implement a least-privilege access model, ensuring that users and services only have access to what is necessary for their roles. In contrast, managing AWS account billing and payment pertains to account management rather than access control. Allowing multiple users access to Amazon EC2 instances focuses on instance access but does not encompass the broader functionality of IAM roles, which is about permissions and security management. Similarly, creating Virtual Private Clouds (VPCs) and managing subnets is related to networking rather than the access delegation and permissions aspects that IAM roles specialize in. Thus, the correct answer emphasizes the

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!