AWS Certified Security Specialty SCS-C02 Practice Test Sample Study Guide

BY EXAMZIFY

EVERYTHING you need from our exam experts!

Featuring practice questions, answers, and explanations for each question.

This study guide is a SAMPLE. Visit https://awscertifiedsecurityspecialty.examzify.com to get the full version available exclusively to Examzify Plus pass holders .

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

Questions

1. **What type of policy can be attached to an Amazon S3 Glacier vault?**

   A. Instance metadata policy

   B. Resource-based vault access policy

   C. User access policy

   D. Network access control policy

2. **Which AWS service is associated with enhancing message delivery reliability?**

   A. Amazon S3

   B. Amazon Simple Notification Service (SNS)

   C. Amazon EC2

   D. AWS Lambda

3. **Which AWS service centrally manages firewall rules across multiple accounts?**

   A. AWS WAF

   B. AWS Network Firewall

   C. AWS Firewall Manager

   D. AWS Certificate Manager (ACM)

4. **Which service encrypts table data before sending it to Amazon DynamoDB?**

   A. Amazon RDS encryption

   B. Amazon EC2 encryption

   C. Amazon DynamoDB Encryption

   D. AWS Key Management Service

5. **What are the two access policy options available for granting permission to Amazon S3 resources?**

   A. IAM roles and instance profiles

   B. Bucket policies and user policies

   C. Security groups and VPCs

   D. User groups and permissions

6. **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**

7. **Which type of S3 Object Lock remains until explicitly removed?**

   A. **Retention Period**

   B. **Legal Hold**

   C. **Governance Mode**

   D. **Compliance Mode**

8. **What is the name of the cryptographic service for maintaining hardware security modules in AWS?**

   A. **AWS Key Management Service**

   B. **AWS CloudHSM**

   C. **AWS Secrets Manager**

   D. **AWS Shield**

9. **Which AWS resource can be used for frequent data updates, such as a database?**

   A. **S3 Bucket**

   B. **EBS Volume**

   C. **EC2 Instance Store**

   D. **AWS Fargate**

10. **What is the primary purpose of applying security patches in a cloud environment?**

    A. **To enhance user accessibility**

    B. **To maintain compliance with industry standards**

    C. **To ensure system software is up to date**

    D. **To increase data storage capacity**

Answers

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

Explanations

1. What type of policy can be attached to an Amazon S3 Glacier vault?

A. Instance metadata policy

B. Resource-based vault access policy

C. User access policy

D. Network access control policy

The type of policy that can be attached to an Amazon S3 Glacier vault is a resource-based vault access policy. This policy is specifically designed to control access permissions for the vault, allowing you to specify who can access data stored in the vault and what actions they can perform. Resource-based vault access policies are crucial for managing data security in Amazon S3 Glacier because they allow you to define permissions at the vault level. This means you can grant or restrict access to specific AWS accounts or IAM users directly on the vault itself, ensuring that only authorized entities can access the data. In contrast, instance metadata policies, user access policies, and network access control policies do not apply specifically to Amazon S3 Glacier vaults. Instance metadata policies are related to instances within EC2, user access policies are typically associated with IAM users and roles, and network access control policies pertain to network resources like security groups or VPC configurations. Thus, these options do not appropriately address the access control mechanisms needed for S3 Glacier vaults.

2. Which AWS service is associated with enhancing message delivery reliability?

A. Amazon S3

B. Amazon Simple Notification Service (SNS)

C. Amazon EC2

D. AWS Lambda

Amazon Simple Notification Service (SNS) is designed specifically to enhance message delivery reliability as it facilitates the reliable delivery of messages to a variety of endpoints. It operates using a publish-subscribe model, allowing messages to be sent to multiple subscribers simultaneously. The service automatically retries delivery to ensure that even if a subscriber is temporarily unavailable, the message will be delivered when they become available again. Moreover, SNS supports various protocols, including HTTP/HTTPS, email, SMS, and even AWS Lambda, enabling flexibility in how notifications are sent and processed. This capability enhances the reliability of message delivery since subscribers can choose the most effective endpoint for their needs. In contrast, while services like Amazon S3, Amazon EC2, and AWS Lambda play important roles in the AWS ecosystem, they do not specifically focus on enhancing message delivery reliability in the same way that SNS does. For example, S3 is primarily a storage service, EC2 is focused on compute resources, and AWS Lambda is a serverless compute service for running code without provisioning servers. Thus, SNS is the most appropriate choice for ensuring reliable message delivery.

3. Which AWS service centrally manages firewall rules across multiple accounts?

A. AWS WAF

B. AWS Network Firewall

C. AWS Firewall Manager

D. AWS Certificate Manager (ACM)

The selected answer, which is AWS Firewall Manager, is the correct choice because this service provides a centralized way to manage and enforce firewall rules across multiple AWS accounts and applications. It enables organizations to apply consistent security policies across various accounts within an AWS Organization, thereby simplifying the management of compliance and security standards. AWS Firewall Manager allows you to configure and manage firewall rules centrally, ensuring that all associated accounts adhere to the defined security policies without requiring individual configuration in each account. This service supports the AWS WAF and AWS Network Firewall, among others, further enhancing its capabilities in a multi-account environment. In contrast, other services mentioned do not serve this centralized management purpose. AWS WAF is a web application firewall that protects web applications by filtering and monitoring HTTP traffic, but it operates at the application level and is not focused on managing rules across multiple accounts. AWS Network Firewall provides network-level security and is designed for use within a single account rather than offering cross-account management. AWS Certificate Manager (ACM) is primarily focused on managing SSL/TLS certificates for securing applications and does not deal with firewall rules at all. Thus, while useful in their respective domains, those services do not provide the centralized management functionality that AWS Firewall Manager does.

4. Which service encrypts table data before sending it to Amazon DynamoDB?

A. Amazon RDS encryption

B. Amazon EC2 encryption

C. Amazon DynamoDB Encryption

D. AWS Key Management Service

Amazon DynamoDB Encryption is specifically designed to encrypt table data before it is sent to the DynamoDB service. This encryption mechanism operates seamlessly, ensuring that data is encrypted at rest and in transit. When you create a DynamoDB table, you can enable encryption, which protects the data using advanced encryption standards, such as AES-256. By using this service, organizations can ensure compliance with various security and data protection regulations. It automatically encrypts all user data, including attributes in items, and maintains strict access controls to ensure only authorized users can interact with the encrypted data. This built-in encryption capability helps safeguard sensitive information and provides peace of mind, allowing developers and businesses to focus on building applications without having to manage encryption manually. The other choices focus on encryption related to different services and contexts, which do not apply directly to the specific task of encrypting data being sent to DynamoDB.

5. What are the two access policy options available for granting permission to Amazon S3 resources?

A. IAM roles and instance profiles

B. Bucket policies and user policies

C. Security groups and VPCs

D. User groups and permissions

The correct option identifies the two access policy mechanisms specifically designed for controlling permissions related to Amazon S3 resources: bucket policies and user policies. Bucket policies are resource-based policies attached directly to an S3 bucket. They define permissions for actions on the bucket and its contents, specifying which AWS accounts or IAM users have access and what actions they can perform. This allows for granular control over who can read, write, or manage the bucket and its objects, down to specific conditions or IP address restrictions. User policies, on the other hand, are identity-based policies that are associated with IAM users, groups, or roles. These policies define what resources a user or group can access and what actions they are allowed to perform on those resources. In the context of S3, user policies can specify permissions for different S3 operations, thereby allowing fine-tuned access control based on the needs of individual users or groups. Together, bucket policies and user policies offer a comprehensive means of managing access to S3 resources, ensuring that permissions can be effectively controlled at both the bucket and user levels. This dual mechanism is essential for maintaining security and operational integrity in an AWS environment.

6. 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.

7. Which type of S3 Object Lock remains until explicitly removed?

A. Retention Period

B. Legal Hold

C. Governance Mode

D. Compliance Mode

The type of S3 Object Lock that remains until explicitly removed is the Legal Hold. A Legal Hold is used when there is a need to preserve data for legal or compliance reasons and does not have a defined retention period. It can only be removed through an explicit action, making it essential for situations where data must be safeguarded against any modifications or deletions until a predetermined condition is met or until a legal directive is lifted. In contrast, the other types of Object Lock have different characteristics. Retention Period specifies a duration during which an object is protected from deletion, and once this period expires, the object can be deleted or modified. Governance Mode allows users with specific permissions to alter or delete objects, while Compliance Mode ensures that objects cannot be deleted or altered for the specified retention period, but it doesn't provide the indefinite hold that a Legal Hold does.

8. What is the name of the cryptographic service for maintaining hardware security modules in AWS?

A. AWS Key Management Service

B. AWS CloudHSM

C. AWS Secrets Manager

D. AWS Shield

AWS CloudHSM is the correct answer as it specifically provides a managed hardware security module (HSM) service that enables customers to generate and use their own encryption keys on the AWS Cloud. This service allows organizations to maintain control over their cryptographic keys and perform cryptographic operations using hardware security modules that comply with industry standards. CloudHSM is particularly valuable for applications that require sensitive data protection while also ensuring compliance with regulatory requirements for key management. Users can integrate CloudHSM with their existing applications to achieve secure key storage while benefiting from the scalability and reliability of the AWS infrastructure. In contrast, while AWS Key Management Service (KMS) is also involved in key management and encryption, it operates in a different manner by providing a fully managed service for creating and controlling encryption keys without directly involving hardware security modules. AWS Secrets Manager is used for managing sensitive information such as API keys and passwords, and AWS Shield is a managed DDoS protection service. Therefore, these services do not offer the same capabilities for managing hardware security modules as AWS CloudHSM does.

9. Which AWS resource can be used for frequent data updates, such as a database?

A. S3 Bucket

B. EBS Volume

C. EC2 Instance Store

D. AWS Fargate

An EBS (Elastic Block Store) Volume is designed to provide persistent block storage for Amazon EC2 instances. It functions like a hard drive that can be attached to EC2 instances, allowing you to store and update data frequently. This is particularly important for databases, which require fast and reliable access to data to handle a high rate of read and write operations.   EBS volumes offer features such as snapshots, which can be used for backups and disaster recovery, as well as the ability to resize volumes as data storage needs grow. They are optimized for performance and are capable of handling I/O-intensive workloads, making them ideal for use cases like databases that require consistent and low-latency data access. In contrast, while S3 Buckets are excellent for storing large amounts of unstructured data and can be used for static website content, they are not suitable for applications that require frequent updates. EC2 Instance Store offers temporary storage that persists only during the lifespan of the instance, making it unsuitable for data that needs to be retained after an instance stops or terminates. AWS Fargate is a serverless compute engine for containers but doesn't directly provide storage capabilities; it works with storage services, rather than operating as a storage resource itself.

10. What is the primary purpose of applying security patches in a cloud environment?

A. To enhance user accessibility

B. To maintain compliance with industry standards

C. To ensure system software is up to date

D. To increase data storage capacity

Applying security patches in a cloud environment primarily serves the purpose of ensuring that system software is up to date. Keeping software up to date is crucial for protecting against vulnerabilities that could be exploited by attackers. Security patches often address known security weaknesses or bugs that, if left unpatched, could lead to unauthorized access, data breaches, or other security incidents. When a patch is released, it typically contains fixes for vulnerabilities that have been discovered after the initial software release. Regularly applying these patches helps in maintaining the integrity and security of the system by closing security gaps and reinforcing defenses against potential threats. While maintaining compliance with industry standards is important and can be influenced by patch management practices, the direct action of applying security patches primarily focuses on the current state of the software rather than the broader compliance landscape. Enhancing user accessibility and increasing data storage capacity are not relevant to the fundamental objective of patching, which is to ensure security and protect the system from known risks.