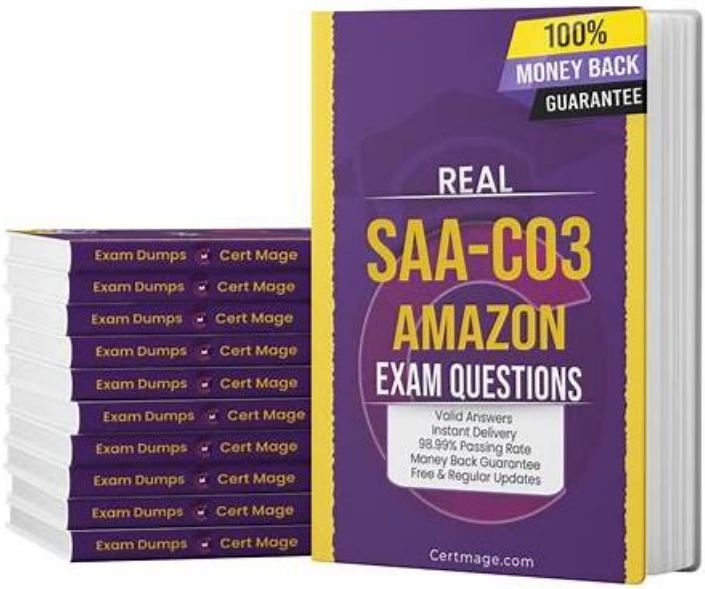
New Launch SCS-C03 PDF Dumps [2026] - Amazon SCS-C03 Exam Questions



BONUS!!! Download part of ExamsReviews SCS-C03 dumps for free: https://drive.google.com/open?id=1-vjuYua1L0Rrts15SxnOjfkMZh7lsjWm

As is known to all, SCS-C03 practice guide simulation plays an important part in the success of exams. By simulation, you can get the hang of the situation of the real exam with the help of our free demo. Simulation of our SCS-C03 training materials make it possible to have a clear understanding of what your strong points and weak points are and at the same time, you can learn comprehensively about the SCS-C03 Exam. By combining the two aspects, you are more likely to achieve high grades.

Amazon SCS-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	• Data Protection: This domain centers on protecting data at rest and in transit through encryption, key management, data classification, secure storage, and backup mechanisms.
Topic 2	• Incident Response: This domain addresses responding to security incidents through automated and manual strategies, containment, forensic analysis, and recovery procedures to minimize impact and restore operations.
Topic 3	• Infrastructure Security: This domain focuses on securing AWS infrastructure including networks, compute resources, and edge services through secure architectures, protection mechanisms, and hardened configurations.

>> Exam SCS-C03 Reviews <<

Amazon SCS-C03 Accurate Study Material | Cheap SCS-C03 Dumps

There have many shortcomings of the traditional learning methods. If you choose our SCS-C03 test training, the intelligent system will automatically monitor your study all the time. Once you study our SCS-C03 certification materials, the system begins to record your exercises. Also, the windows software will automatically generate a learning report when you finish your practices of the SCS-C03 Real Exam dumps, which helps you to adjust your learning plan. It is crucial that you have formed a correct review method. The role of our SCS-C03 test training is optimizing and monitoring your study. Sometimes you have no idea about your problems. So you need our SCS-C03 real exam dumps to promote your practices.

Amazon AWS Certified Security - Specialty Sample Questions (Q126-Q131):

NEW QUESTION # 126
A company's data scientists want to create artificial intelligence and machine learning (AI/ML) training models by using Amazon SageMaker. The training models will use large datasets in an Amazon S3 bucket. The datasets contain sensitive information.
On average, the data scientists need 30 days to train models. The S3 bucket has been secured appropriately. The company's data retention policy states that all data that is older than 45 days must be removed from the S3 bucket.
Which action should a security engineer take to enforce this data retention policy?

- A. Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an Amazon EventBridge rule to invoke the Lambda function each month.
- B. Configure an S3 Lifecycle rule on the S3 bucket to delete objects after 45 days.
- C. Create an AWS Lambda function to check the last-modified date of the S3 objects and delete objects that are older than 45 days. Create an S3 event notification to invoke the Lambda function for each PutObject operation.
- D. Configure S3 Intelligent-Tiering on the S3 bucket to automatically transition objects to another storage class.

Answer: B

Explanation:
Amazon S3 Lifecycle rules provide a native, fully managed mechanism to automatically transition or delete objects based on their age. According to the AWS Certified Security - Specialty Official Study Guide, S3 Lifecycle policies are the recommended and most secure method for enforcing data retention requirements because they operate automatically, consistently, and without custom code.
By configuring a lifecycle rule to delete objects after 45 days, the company ensures that sensitive datasets are retained long enough to support the 30-day model training process while remaining compliant with the data retention policy. Lifecycle rules are enforced by Amazon S3 itself and apply uniformly to all objects in the bucket or to objects that match specific prefixes or tags.

NEW QUESTION # 127
A company allows users to download its mobile app onto their phones. The app is MQTT based and connects to AWS IoT Core to subscribe to specific client-related topics. Recently, the company discovered that some malicious attackers have been trying to get a Trojan horse onto legitimate mobile phones. The Trojan horse poses as the authentic application and uses a client ID with injected special characters to gain access to topics outside the client ' s privilege scope.
Which combination of actions should the company take to prevent this threat? (Select TWO.)

- A. Apply an AWS IoT Core policy to the device to allow " iot:Connect " with the resource set to " client /${iot:Connection.Thing.ThingName} ".
- B. In the application, use an IoT thing name as the client ID to connect the device to AWS IoT Core.
- C. In the application, add a client ID check. Disconnect from the server if any special character is detected.
- D. Apply an AWS IoT Core policy to the device to allow " iot:Connect " with the resource set to " client /${iot:ClientId} ".
- E. Apply an AWS IoT Core policy that allows " AWSIoTWirelessDataAccess " with the principal set to " client/${iot:Connection.Thing.ThingName} ".

Answer: A,B

Explanation:
The threat is client ID manipulation to break authorization boundaries. The strongest control is tobind the MQTT client identity to the authenticated device identity(the Thing) rather than trusting arbitrary client IDs provided by the client. Using theThing name as the client ID(Option A) removes ambiguity and makes the identifier predictable and tied to a registered identity.
On the authorization side, AWS IoT Core policies can use policy variables. Allowing iot:Connect only when the resource matches client/${iot:Connection.Thing.ThingName} (Option E) ensures the connection is permittedonlyif the client ID exactly equals the authenticated Thing name from the TLS certificate/Thing principal context. This prevents attackers from injecting special characters or choosing a different client ID to escalate access, because the policy evaluation ties the allowed client resource to the Thing

identity, not the attacker-controlled string.
Option D is weaker because it effectively allows whatever client ID is presented (it matches the same value the client supplies), so it does not prevent crafted client IDs from being used. Option C is unrelated to the described MQTT connect authorization (and references an action not aligned with the scenario). Option B is an application-side check and can be bypassed by a malicious client; enforcement must be at AWS IoT Core policy level.

NEW QUESTION # 128
A company recently set up Amazon GuardDuty and is receiving a high number of findings from IP addresses within the company. A security engineer has verified that these IP addresses are trusted and allowed.
Which combination of steps should the security engineer take to configure GuardDuty so that it does not produce findings for these IP addresses? (Select TWO.)

- A. Create a JSON configuration file that contains the trusted IP addresses.
- B. Upload the configuration file to Amazon S3. Add a new trusted IP list to GuardDuty that points to the file.
- C. Manually copy and paste the configuration file data into the trusted IP list in GuardDuty.
- D. Create a plaintext configuration file that contains the trusted IP addresses.
- E. Upload the configuration file directly to GuardDuty.

Answer: B,D

Explanation:
GuardDuty supports "Trusted IP lists" to suppress findings that would otherwise be generated for activity originating from known safe IP addresses (for example, corporate NAT egress IPs, security scanners, or monitoring systems). To use a trusted IP list, you create aplain textfile that contains the IP addresses (typically one per line or in supported list form) and store it inAmazon S3. You then configure GuardDuty to reference that S3 object as a trusted IP list. GuardDuty periodically retrieves the file from S3 and uses it to adjust finding generation accordingly.
That maps directly to Option A (create a plaintext file) and Option D (upload to S3 and create a trusted IP list in GuardDuty pointing to the file).
Options B and E are incorrect because GuardDuty trusted IP lists are not configured by pasting JSON into the console; they are sourced from an S3-hosted text list. Option C is not supported because GuardDuty does not accept direct file uploads into the service as the configuration source; S3 is the expected integration point for IP lists and threat intel lists.

NEW QUESTION # 129
A company needs centralized log monitoring with automatic detection across hundreds of AWS accounts. Which solution meets these requirements with the LEAST operational effort?

- A. Designate a GuardDuty administrator account and enable protections.
- B. Centralize CloudTrail logs and query with Athena.
- C. Stream logs to Kinesis and process with Lambda.
- D. Centralize CloudWatch logs and use Inspector.

Answer: A

Explanation:
Amazon GuardDuty provides fully managed threat detection across accounts when configured with delegated administration. EKS and RDS protections enable workload-aware detection with minimal setup.
Other solutions require custom pipelines and higher operational overhead.

NEW QUESTION # 130
A company uses Amazon API Gateway to present REST APIs to users. An API developer wants to analyze API access patterns without the need to parse the log files.
Which combination of steps will meet these requirements with the LEAST effort? (Select TWO.)

- A. Select the Enable Detailed CloudWatch Metrics option on the required API stage.
- B. Configure an Amazon S3 destination for API Gateway logs. Run Amazon Athena queries to analyze API access information.
- C. Configure an AWS CloudTrail trail destination for API Gateway events. Configure filters on the userIdentity, userAgent,

and sourceIPAddress fields.

- D. Configure access logging for the required API stage.
- E. Use Amazon CloudWatch Logs Insights to analyze API access information.

Answer: A,E

Explanation:
To analyze API access patterns with minimal effort andwithout parsing raw log files, the best approach is to rely onmetricsand built-in query tooling. EnablingDetailed CloudWatch Metricsfor an API Gateway stage (Option E) provides near-real-time, aggregated visibility into usage and performance patterns (such as request counts, latency, error rates like 4XX/5XX) that are ideal for identifying trends and spikes without handling logs.
For deeper pattern exploration when needed,CloudWatch Logs Insights(Option D) provides an interactive query experience over logs that are already in CloudWatch Logs, allowing quick filtering and aggregation. In practice, developers use metrics to understand access patterns at a high level and Logs Insights to slice and dice request data without building a separate parsing pipeline.
Options A and C still rely on enabling access logs and shipping them to S3/Athena, which is more setup and operational overhead (and still involves managing log storage/format). CloudTrail (Option B) records control- plane API calls to AWS services, not end-user access requests to your API methods, so it won't provide the desired access pattern view for API consumers. Therefore, Detailed CloudWatch Metrics plus CloudWatch Logs Insights is the least-effort combination for access pattern analysis.

NEW QUESTION # 131
.....

P.S. Free & New SCS-C03 dumps are available on Google Drive shared by ExamsReviews: https://drive.google.com/open?id=1-vjuYua1L0Rrts15SxnOjfkMZh7lsjWm