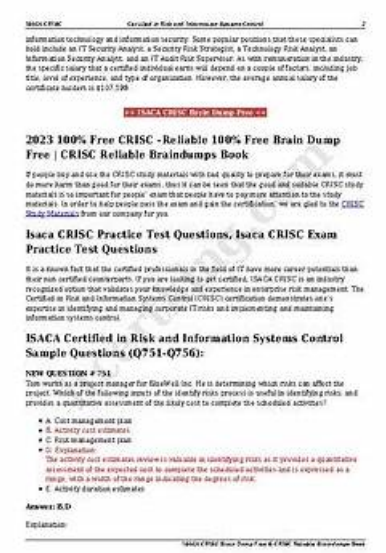
Reliable SCS-C03 Dumps Sheet - Latest Braindumps SCS-C03 Book



2023 100% Free CRISC -Reliable 100% Free Brain Dump Free | CRISC Reliable Braindumps Book

Isaca CRISC Practice Test Questions, Isaca CRISC Exam Practice Test Questions

ISACA Certified in Risk and Information Systems Control Sample Questions (Q751-Q756):

The passing rate of our SCS-C03 training quiz is 99% and the hit rate is also high. Our professional expert team seizes the focus of the exam and chooses the most important questions and answers which has simplified the important SCS-C03 information and follow the latest trend to make the client learn easily and efficiently. We update the SCS-C03 Study Materials frequently to let the client practice more. We provide the function to stimulate the SCS-C03 exam and the timing function of our SCS-C03 study materials to adjust your speed to answer the questions. You will pass the SCS-C03 exam easily.

It is apparent that a majority of people who are preparing for the SCS-C03 exam would unavoidably feel nervous as the exam approaching, since you have clicked into this website, you can just take it easy now--our SCS-C03 learning materials. Our company has spent more than 10 years on compiling study materials for the exam, and now we are delighted to be here to share our SCS-C03 Study Materials with all of the candidates for the exam in this field. There are so many striking points of our SCS-C03 preparation exam.

>> Reliable SCS-C03 Dumps Sheet <<

100% Pass-Rate Reliable SCS-C03 Dumps Sheet Offer You The Best Latest Braindumps Book | Amazon AWS Certified Security - Specialty

If you really intend to pass the SCS-C03 exam, our software will provide you the fast and convenient learning and you will get the

best study materials and get a very good preparation for the exam. The content of the SCS-C03 guide torrent is easy to be mastered and has simplified the important information. What's more, our SCS-C03 prep torrent conveys more important information with less questions and answers. The learning is relaxed and highly efficiently.

Amazon SCS-C03 Exam Syllabus Topics:

Topic	Details
Topic 1	• Detection: This domain covers identifying and monitoring security events, threats, and vulnerabilities in AWS through logging, monitoring, and alerting mechanisms to detect anomalies and unauthorized access.
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	• Identity and Access Management: This domain deals with controlling authentication and authorization through user identity management, role-based access, federation, and implementing least privilege principles.

Amazon AWS Certified Security - Specialty Sample Questions (Q30-Q35):

NEW QUESTION # 30
A company must inventory sensitive data across all Amazon S3 buckets in all accounts from a single security account.

- A. Use Macie with Trusted Advisor.
- B. Use Inspector with Trusted Advisor.
- C. Use Amazon Inspector with Security Hub.
- D. Delegate Amazon Macie and Security Hub administration.

Answer: D

Explanation:
Amazon Macie is the AWS service designed to discover and classify sensitive data in S3.
Delegated administration enables centralized visibility across an organization. Security Hub aggregates Macie findings for a single-pane-of-glass view.
Inspector does not scan S3 data. Trusted Advisor is not a sensitive data discovery tool.

NEW QUESTION # 31
A security engineer is designing a solution that will provide end-to-end encryption between clients and Docker containers running in Amazon Elastic Container Service (Amazon ECS). This solution must also handle volatile traffic patterns. Which solution would have the MOST scalability and LOWEST latency?

- A. Configure an Application Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
- B. Configure a Network Load Balancer to terminate the TLS traffic and then re-encrypt the traffic to the containers.
- C. Configure a Network Load Balancer with a TCP listener to pass through TLS traffic to the containers.
- D. Configure Amazon Route 53 to use multivalue answer routing to send traffic to the containers.

Answer: C

Explanation:
Network Load Balancers operate at Layer 4 and are optimized for extreme performance, ultra-low latency, and handling sudden traffic spikes. According to AWS Certified Security - Specialty documentation, using a TCP listener on an NLB allows TLS traffic to pass through directly to backend containers without termination, preserving true end-to-end encryption.
This approach eliminates the overhead of decrypting and re-encrypting traffic at the load balancer, reducing latency and maximizing throughput. NLBs scale automatically to handle volatile traffic patterns and millions of requests per second.
Application Load Balancers operate at Layer 7 and introduce additional latency due to TLS termination and HTTP processing.
Route 53 multivalue routing does not provide load balancing at the transport layer and does not ensure encryption handling.
AWS recommends NLB TCP pass-through for high-performance, end-to-end encrypted container workloads.

NEW QUESTION # 32
A company has several Amazon S3 buckets that do not enforce encryption in transit. A security engineer must implement a solution that enforces encryption in transit for all the company's existing and future S3 buckets. Which solution will meet these requirements?

- A. Enable AWS Config. Create a proactive AWS Config Custom Policy rule. Create a Guard clause to evaluate the S3 bucket policies to check for a value of True for the aws:SecureTransport condition key. If the AWS Config rule evaluates to NON_COMPLIANT, block resource creation.
- B. Enable AWS Config. Configure the s3-bucket-ssl-requests-only AWS Config managed rule and set the rule trigger type to Hybrid. Create an AWS Systems Manager Automation runbook that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is False. Configure automatic remediation. Set the runbook as the target of the rule.
- C. Enable Amazon Inspector. Create a custom AWS Lambda rule. Create a Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is False. Set the Lambda function as the target of the rule.
- D. Create an AWS CloudTrail trail. Enable S3 data events on the trail. Create an AWS Lambda function that applies a bucket policy to deny requests when the value of the aws:SecureTransport condition key is False. Configure the CloudTrail trail to invoke the Lambda function.

Answer: B

Explanation:
To enforce encryption in transit for Amazon S3, AWS best practice is to require HTTPS (TLS) by using a bucket policy condition that denies any request where aws:SecureTransport is false. The requirement includes both existing buckets and future buckets, so the control must continuously evaluate configuration drift and automatically remediate. AWS Config is the service intended for continuous configuration compliance monitoring across resources, and AWS Config managed rules provide standardized checks with low operational overhead. The s3-bucket-ssl-requests- only managed rule evaluates whether S3 buckets enforce SSL-only requests, aligning directly with enforcing encryption in transit. Setting the trigger type to Hybrid ensures evaluation both on configuration changes and periodically. Automatic remediation with an AWS Systems Manager Automation runbook allows the organization to apply or correct the bucket policy consistently at scale without manual work. This approach also supports governance by maintaining a measurable compliance status while actively fixing noncompliance. Option A is not the best fit because a "proactive" custom policy rule does not by itself remediate existing buckets and "block resource creation" is not how AWS Config enforces controls. Option C is incorrect because Amazon Inspector is a vulnerability management service and does not govern S3 bucket transport policies. Option D is inefficient and indirect because CloudTrail data events are not a compliance engine and would require custom processing.

NEW QUESTION # 33
A company's application team needs a new AWS Key Management Service (AWS KMS) customer managed key to use with Amazon S3. The company's security policy requires separate keys for different AWS services to limit security exposure. How can a security engineer limit the KMS customer managed key to work with only Amazon S3?

- A. Configure the key policy to allow only Amazon S3 to perform the kms:Encrypt action.
- B. Configure the application's IAM role policy to allow only S3 operations when the operations are combined with the KMS customer managed key.
- C. Configure the key policy to allow KMS actions only when the value for the kms:ViaService condition key matches the Amazon S3 service name.
- D. Configure the application's IAM role policy to allow Amazon S3 to perform the iam:PassRole action.

Answer: C

Explanation:
AWS KMS provides condition keys that can be used to tightly scope how and where a customer managed key can be used. According to the AWS Certified Security - Specialty Study Guide, the kms:ViaService condition key is specifically designed to restrict key usage to requests that originate from a particular AWS service in a specific Region.
By configuring the key policy to allow KMS cryptographic operations only when kms:ViaService equals s3.<region>.amazonaws.com, the security engineer ensures that the key can be used exclusively by Amazon S3. Even if other IAM principals have permissions to use the key, the key cannot be used by other services such as Amazon EC2, Amazon RDS, or AWS Lambda.
Option A is incorrect because AWS services do not assume identities in key policies. Options C and D modify IAM role policies, which do not control how a KMS key is used by AWS services.
AWS documentation clearly states that service-level restrictions must be enforced at the KMS key policy level using condition keys.

This approach enforces strong separation of duties and limits blast radius, which aligns with AWS security best practices.

NEW QUESTION # 34
A company is using Amazon Macie, AWS Firewall Manager, Amazon Inspector, and AWS Shield Advanced in its AWS account. The company wants to receive alerts if a DDoS attack occurs against the account.
Which solution will meet this requirement?

- A. Create an Amazon CloudWatch alarm that monitors AWS Shield Advanced metrics for an active DDoS event.
- B. Use Amazon Inspector to review resources and invoke Amazon CloudWatch alarms for any resources that are vulnerable to DDoS attacks.
- C. Use Amazon Macie to detect an active DDoS event and create Amazon CloudWatch alarms that respond to Macie findings.
- D. Create an Amazon CloudWatch alarm that monitors AWS Firewall Manager metrics for an active DDoS event.

Answer: A

Explanation:
AWS Shield Advanced is the AWS-native managed service specifically designed to provide detection, mitigation, and visibility for Distributed Denial of Service (DDoS) attacks at both the network and application layers. Shield Advanced integrates directly with Amazon CloudWatch by publishing DDoS-related metrics such as DDoSDetected, AttackVolume, and AttackVector, which can be monitored using CloudWatch alarms to trigger alerts in near real time. This makes option D the correct and fully supported solution.
Amazon Macie focuses on discovering and protecting sensitive data (such as PII) in Amazon S3 using machine learning and does not provide DDoS detection capabilities, making option A incorrect. Amazon Inspector is a vulnerability management service that assesses EC2 instances, container images, and Lambda functions for software vulnerabilities and unintended network exposure; it does not detect live DDoS attacks, so option B is incorrect. AWS Firewall Manager is a centralized management service for configuring AWS WAF, Shield Advanced, and security groups across accounts, but it does not emit native DDoS detection metrics for alerting, which eliminates option C.
According to AWS Security Specialty documentation, the recommended best practice for DDoS detection and alerting is to enable AWS Shield Advanced and configure Amazon CloudWatch alarms on Shield metrics, optionally integrating with Amazon SNS for notifications and AWS Incident Manager for response automation.

NEW QUESTION # 35
.....

Many companies arrange applicants to take certification exams since 1995 internationally such like Microsoft, Fortinet, Veritas, EMC, and HP. Amazon SCS-C03 exam sample online was produced in 2001 and popular in 2008. So far many companies built long-term cooperation with exam dumps providers. Many failure experiences tell them that purchasing a valid Amazon SCS-C03 Exam Sample Online is the best effective and money-cost methods to achieve their goal.

- Free PDF Accurate Amazon - Reliable SCS-C03 Dumps Sheet □ Search for ⇛ SCS-C03 ⇚ and download it for free on [www.testkingpass.com] website □Certified SCS-C03 Questions
- Amazon SCS-C03 Exam | Reliable SCS-C03 Dumps Sheet - One Year Free Updates of Latest Braindumps SCS-C03 Book □ Immediately open ➽ www.pdfvce.com □ and search for ➡ SCS-C03 □□□ to obtain a free download □ □Reliable SCS-C03 Real Exam
- SCS-C03 New Question □ SCS-C03 Pdf Version ✳ SCS-C03 New Question □ Open ▹ www.prep4sures.top ◃ and search for ☀ SCS-C03 □☀□ to download exam materials for free □SCS-C03 Latest Learning Materials
- www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, academy.rebdaa.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, www.stes.tyc.edu.tw, Disposable vapes