SCS-C02 Hot Questions & Exam Discount SCS-C02 Voucher

DOWNLOAD the newest Prep4SureReview SCS-C02 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=16LwExm0TgZPn1TWFCwA_TajUvqgextyU

If your problems on studying the SCS-C02 learning quiz are divulging during the review you can pick out the difficult one and focus on those parts. You can re-practice or iterate the content of our SCS-C02 exam questions if you have not mastered the points of knowledge once. Especially for exam candidates who are scanty of resourceful products, our SCS-C02 study prep can whittle down distention of disagreement and reach whole acceptance.

Amazon SCS-C02 Exam Syllabus Topics:

Topic	Details
Topic 1	• Infrastructure Security: Aspiring AWS Security specialists are trained to implement and troubleshoot security controls for edge services, networks, and compute workloads under this topic. Emphasis is placed on ensuring resilience and mitigating risks across AWS infrastructure. This section aligns closely with the exam's focus on safeguarding critical AWS services and environments.
Topic 2	• Identity and Access Management: The topic equips AWS Security specialists with skills to design, implement, and troubleshoot authentication and authorization mechanisms for AWS resources. By emphasizing secure identity management practices, this area addresses foundational competencies required for effective access control, a vital aspect of the certification exam.
Topic 3	• Threat Detection and Incident Response: In this topic, AWS Security specialists gain expertise in crafting incident response plans and detecting security threats and anomalies using AWS services. It delves into effective strategies for responding to compromised resources and workloads, ensuring readiness to manage security incidents. Mastering these concepts is critical for handling scenarios assessed in the SCS-C02 Exam.
Topic 4	• Management and Security Governance: This topic teaches AWS Security specialists to develop centralized strategies for AWS account management and secure resource deployment. It includes evaluating compliance and identifying security gaps through architectural reviews and cost analysis, essential for implementing governance aligned with certification standards.
Topic 5	• Data Protection: AWS Security specialists learn to ensure data confidentiality and integrity for data in transit and at rest. Topics include lifecycle management of data at rest, credential protection, and cryptographic key management. These capabilities are central to managing sensitive data securely, reflecting the exam's focus on advanced data protection strategies.

2026 SCS-C02 Hot Questions | Professional AWS Certified Security - Specialty 100% Free Exam Discount Voucher

Working in IT field, you definitely want to prove your ability by passing IT certification test. Moreover, the colleagues and the friends with IT certificate have been growing. In this case, if you have none, you will not be able to catch up with the others. For example like Amazon SCS-C02 Certification Exam, it is a very valuable examination, which must help you realize your wishes.

Amazon AWS Certified Security - Specialty Sample Questions (Q312-Q317):

NEW QUESTION # 312
A company is planning to deploy a new log analysis environment. The company needs to implement a solution to analyze logs from multiple AWS services in near real time. The solution must provide the ability to search the logs. The solution also must send alerts to an existing Amazon Simple Notification Service (Amazon SNS) topic when specific logs match detection rules.
Which solution will meet these requirements?

- A. Analyze the logs by using Amazon OpenSearch Service. Search the logs from the OpenSearch API.
  Use OpenSearch Service Security Analytics to match logs with detection rules and to send alerts to the SNS topic.
- B. Analyze the logs by using Amazon QuickSight. Search the logs by listing the query results in a dashboard. Run queries to match logs with detection rules and to send alerts to the SNS topic.
- C. Analyze the logs by using Amazon CloudWatch Logs. Use a subscription filter to match logs with detection rules and to send alerts to the SNS topic. Search the logs manually by using CloudWatch Logs Insights.
- D. Analyze the logs by using AWS Security Hub. Search the logs from the Findings page in Security Hub.
  Create custom actions to match logs with detection rules and to send alerts to the SNS topic.

Answer: A

Explanation:
Amazon OpenSearch Service provides near real-time log ingestion and indexing, full-text search, and analytics capabilities. Using the Security Analytics feature, you can define detection rules and configure alerts based on log patterns or threat indicators. These alerts can be routed to Amazon SNS topics for notification and automation workflows.
This meets the requirements for:
Near real-time log ingestion and search
Rule-based detection and alerting
Integration with SNS for notifications
This solution aligns with best practices under the Logging and Monitoring domain in the AWS Certified Security - Specialty curriculum.

NEW QUESTION # 313
An international company wants to combine AWS Security Hub findings across all the company's AWS Regions and from multiple accounts. In addition, the company wants to create a centralized custom dashboard to correlate these findings with operational data for deeper analysis and insights. The company needs an analytics tool to search and visualize Security Hub findings.
Which combination of steps will meet these requirements? (Chose three.)

- A. Designate an AWS account as a delegated administrator for Security Hub. Publish events to Amazon CloudWatch from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings.
- B. In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis data stream. Configure the Kinesis data streams to output the logs to a single Amazon S3 bucket.
- C. Designate an AWS account in an organization in AWS Organizations as a delegated administrator for Security Hub. Publish events to Amazon EventBridge from the delegated administrator account, all member accounts, and required Regions that are enabled for Security Hub findings.
- D. In each Region, create an Amazon EventBridge rule to deliver findings to an Amazon Kinesis Data Firehose delivery stream. Configure the Kinesis Data Firehose delivery streams to deliver the logs to a single Amazon S3 bucket.
- E. Use AWS Glue DataBrew to crawl the Amazon S3 bucket and build the schema. Use AWS Glue Data Catalog to query the data and create views to flatten nested attributes. Build Amazon QuickSight dashboards by using Amazon Athena.
- F. Partition the Amazon S3 data. Use AWS Glue to crawl the S3 bucket and build the schema. Use Amazon Athena to query the data and create views to flatten nested attributes. Build Amazon QuickSight dashboards that use the Athena views.

Answer: C,D,F

Explanation:
https://aws.amazon.com/blogs/architecture/visualize-aws-security-hub-findings-using-analytics- and-business-intelligence-tools/

NEW QUESTION # 314
A company sends Amazon RDS snapshots to two accounts as part of its disaster recovery (DR) plan. The snapshots must be encrypted. However, each account needs to be able to decrypt the snapshots in case of a DR event.
Which solution will meet these requirements?

- A. Use an AWS Key Management Service (AWS KMS) customer managed key to generate the snapshots. Share the KMS key with the two accounts by using an IAM principal that has the proper KMS permissions in each account.
- B. Use the default AWS Key Management Service (AWS KMS) key to generate the snapshots.
  Create an AWS Lambda function that copies the KMS encryption key to the two accounts.
- C. Use the default AWS Key Management Service (AWS KMS) key to generate the snapshots.
  Share the KMS key with the two accounts by using an IAM principal that has the proper KMS permissions in each account.
- D. Use an AWS Key Management Service (AWS KMS) customer managed key to generate the snapshots. Create an AWS Lambda function that imports the KMS key in the two accounts.

Answer: A

Explanation:
Amazon Relational Database Service (Amazon RDS) can encrypt data using an AWS managed key or a Customer managed key (CMK). Key permissions fully integrate with AWS Identity and Access Management (IAM).
https://aws.amazon.com/blogs/database/securing-data-in-amazon-rds-using-aws-kms-encryption/
https://aws.amazon.com/premiumsupport/knowledge-center/share-encrypted-rds-snapshot-kms- key/

NEW QUESTION # 315
A company's data scientists want to create AI/ML training models 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 older than 45 days must be removed from the S3 bucket.

- A. Configure S3 Intelligent-Tiering on the S3 bucket to automatically transition objects to another storage class.
- 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. 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.

Answer: B

Explanation:
Comprehensive Detailed Explanation with all AWS References
The simplest and most efficient way to enforce a data retention policy in Amazon S3 is by using S3 Lifecycle rules:
* S3 Lifecycle Rule:
* Lifecycle rules allow you to automatically delete objects based on their age or last-modified date.
* Specify a rule to delete objects after 45 days to meet the retention policy.

NEW QUESTION # 316
To meet regulatory requirements, a Security Engineer needs to implement an IAM policy that restricts the use of AWS services to the us-east-1 Region.
What policy should the Engineer implement?

- A.
- B. A computer code with black text Description automatically generated
- C. A computer code with text Description automatically generated

- D. A computer code with black text Description automatically generated

Answer: D

Explanation:
https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_examples_aws_deny-requested- region.html

NEW QUESTION # 317
......

We will definitely not live up to the trust of users in our SCS-C02 study materials. As you know, the users of our SCS-C02 exam questions are all over the world. We have also been demanding ourselves with the highest international standards to support our SCS-C02 training guide in every aspect. First of all, our system is very advanced and will not let your information leak out. It is totally safe to visit our website and buy our SCS-C02 learning prep. You won't worry anything with our services.

Exam Discount SCS-C02 Voucher: https://www.prep4surereview.com/SCS-C02-latest-braindumps.html

2026 Latest Prep4SureReview SCS-C02 PDF Dumps and SCS-C02 Exam Engine Free Share: https://drive.google.com/open?id=16LwExm0TgZPn1TWFCwA_TajUvqgextyU